CONVENTIONAL FORCES INTELLIGENCE AND ARMY SPECIAL OPERATIONS FORCES, SPECIFICALLY SPECIAL FORCES, INTERCONNECTIVITY IN FORCE XXI

A Thesis presented to the Faculty of the U.S. Army Command and General Staff College in partial fulfillment of the requirements for the degree

MASTER OF MILITARY ART AND SCIENCE

by

Steven T. Shoemaker, MAJ, U.S. Army
B.A., Fresno State College, California
1979

Fort Leavenworth, Kansas
1997

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	7 June 1997	Master's Thesis, 2 Aug 96 - 7 June 1997

4. TITLE AND SUBTITLE
Interconnectivity of Special Operations Forces, Specifically Special Forces, and Conventional Force Intelligence Systems in Force XXI TITLE ON COVER & CONVENTIONAL FORCES INTELLIGENCE AND ARMY SPECIAL OPERATIONS FORCES, SPECIFICALLY SPECIAL FORCES, INTERCONNECTIVITY IN FORCE XXI

5. FUNDING NUMBERS

6. AUTHOR(S)
Major Steven T. Shoemaker, U.S. Army

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
Fort Leavenworth, Kansas 66027-1352

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*
The United States Army is focusing its future on researching, developing, and the acquisition of equipment for a concept called Force XXI. In this new concept, the Army plans to collect and share information using mostly electronic sensors via satellite communications to interconnect computers. Emerging information and digital technology will create a synergistic effect among weapons, organizations, and components that will significantly enhance the Army's capabilities. Force XXI will focus on using seamless connectivity to dominate the enemy speed, space, and time. As one of the few human sensors, Army special operations forces (ARSOF) interconnect withe Army conventional forces (CF) and other Department of Defense (DoD) services. The thesis question is: will special forces (SF) teams be seamlessly connected to the intelligence systems of Army conventional forces in Force XXI? By researching the futurists' view of the twenty-first century, the inception of Force XXI, the concept of Force XXI, the Army's Concepts Based Requirements System, the inception of Force XXI, the concept of Force XXI,, and US Army Special Operations Command plans for intelligence interconnectivity in the twenty-first century, the author analyzed and synthesized a substantial amount of information in order to produce a summary of concept and linkage. From the research the author concluded that the intelligence systems of ARSOF, specifically SF, and the U.S. Army CF will not be interconnected in Force XXI.

14. SUBJECT TERMS
Force XXI, Interconnectivity, Special Forces, Conventional Forces

15. NUMBER OF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED

CONVENTIONAL FORCES INTELLIGENCE AND ARMY SPECIAL OPERATIONS FORCES, SPECIFICALLY SPECIAL FORCES, INTERCONNECTIVITY IN FORCE XXI

A Thesis presented to the Faculty of the U.S. Army Command and General Staff College in partial fulfillment of the requirements for the degree

MASTER OF MILITARY ART AND SCIENCE

by

Steven T. Shoemaker, MAJ, U.S. Army
B.A., Fresno State College, California
1979

Fort Leavenworth, Kansas
1997

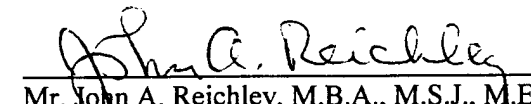
MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

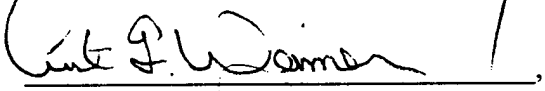
Name of Candidate: MAJ Steven T. Shoemaker, U.S. Army

Thesis Title: Conventional Forces Intelligence and Army Special Operations Forces, Specifically Special Forces, Interconnectivity in Force XXI

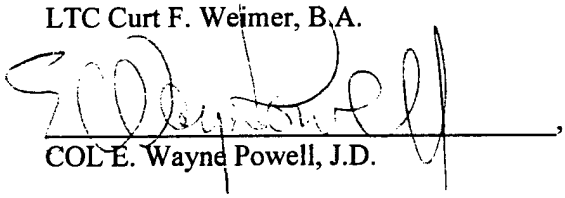
Approved by:



_____, Thesis Committee Chairman
Mr. John A. Reichley, M.B.A., M.S.J., M.Ed.

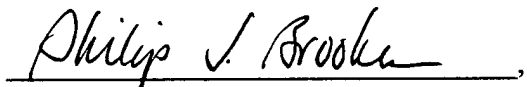


_____, Member
LTC Curt F. Weimer, B.A.



_____, Member, Consulting Faculty
COL E. Wayne Powell, J.D.

Accepted this 6th day of June 1997 by:



_____, Director, Graduate Degree Programs
Philip J. Brookes, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study include the following statement.)

ABSTRACT

INTERCONNECTIVITY OF SPECIAL OPERATIONS FORCES, SPECIFICALLY SPECIAL FORCES, AND CONVENTIONAL FORCE INTELLIGENCE SYSTEMS IN FORCE XXI, by Major Steven T. Shoemaker, U.S. Army, 93 pages.

The United States Army is focusing its future on researching, developing, and the acquisition of equipment for a concept called Force XXI. In this new concept, the Army plans to collect and share information using mostly electronic sensors via satellite communications to interconnect computers. Emerging information and digital technology will create a synergistic effect among weapons, organizations, and components that will significantly enhance the Army's capabilities. Force XXI will focus on using seamless connectivity to dominate the enemy speed, space, and time. As one of the few human sensors, Army special operations forces (ARSOF) interconnect with Army conventional forces (SF) teams be seamlessly connected to the intelligence systems of Army conventional forces in Force XXI? By researching the futurists' view of the twenty-first century, the inception of Force XXI, the concept of Force XXI, the Army's Concepts Based Requirements System, the Intelligence XXI concept, and US Army Special Operations Command plans for intelligence interconnectivity in the twenty-first century, the author analyzed and synthesized a substantial amount of information in order to produce a summary of concept and linkage. From the research the author concluded that the intelligence systems of ARSOF, specifically SF, and US Army CF will not be interconnected in Force XXI.

ACKNOWLEDGEMENTS

This thesis would not have been started at all if not for two intelligence experts, each in different headquarters: Mr. Jerry Reinhole, USASOC DCSINT, was invaluable for explaining the intricacies and history of the ARSOF/CF relationship; and Mr. Rod Ritter who patiently helped me gain a more thorough understanding of file transfer while providing large amounts of information about the CF view of the intelligence world. Of most importance to the actual completion of the thesis is my wife, Vicki. She volunteered to type raw information into the computer while I continued Command and General Staff College requirements and further research. It is not certain that she really knew what an involved process it would become, but she persevered until there existed over one hundred pages of single-spaced information that sometimes only remotely applied to the thesis. Without her this thesis would truly not have advanced to completion. And finally, without the help of Vaughn Neeld, editor extraordinaire, this thesis would probably be in the waste basket. It is only through her help that this thesis is coherent to the reader. And finally, thanks to the MMAS committee, who gave me enough freedom to pursue tangents but gently kept me focused on the subject.

TABLE OF CONTENTS

Page

APPROVAL PAGE ii

ABSTRACT iii

ACKNOWLEDGEMENTS iv

LIST OF FIGURES v

LIST OF ABBREVIATIONS vi

CHAPTER

1. INTRODUCTION 1

2. REVIEW OF LITERATURE 11

3. RESEARCH METHODOLOGY 15

4. ANALYSIS 18

5. CONCLUSIONS AND RECOMMENDATIONS 73

BIBLIOGRAPHY 85

INITIAL DISTRIBUTION LIST 93

LIST OF FIGURES

Figure

1. List of Army Systems and Their Information Transfer Speeds 56

2. Quick List of Subordinate Thesis Questions 81

LIST OF ACRONYMS

AAN	Army After Next
ABCS	Army Battle Command System
ACT II	Advanced Concepts and Technology II (second version)
ACTD	Advance Concept Technology Demonstration
AD	Air Defense
ADO	Army Digitization Office
ADMP	Army Digitization Master Plan
ADP	Army Digitization Plan
AFATDS	Advanced Field Artillery Tactical Data System
AGCCS	Army Global Command and Control System
AI	Artificial Intelligence
ALRPG	Army Long Range Planning Guidance
AMO	Army Modernization Objectives
AMP	Army Modernization Plan
ARSOF	Army Special Operations Forces
ASAS	All-Source Analysis System
ASAS II	All-Source Analysis System II (second version)
ASAS II-RWS	All-Source Analysis System (second version)-Remote Workstation
ASAS/SDR	All-Source Analysis System/Surrogate Digital Radio
ASB	Army Science Board

ASDSO-LIC	Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict
ASTMP	Army Science and Technology Master Plan
ATACMS	Army Tactical Missile System
ATCCS	Army Tactical Command and Control System
ATM	Asynchronous Transfer Mode
AWE	Advanced Warfighter Experiment
BADD	Battlefield Awareness and data Dissemination
B2C2	Brigade and Below Command and Control system
BCBL	Battle Command Battle Lab
CA	Civil Affairs
CBRS	Concepts-Based Requirements System
C2	Command and Control
C3	Command, Control, and Communications
C4I	Command, Control, Communications, Computers, and Intelligence
C2W	Command and Control Warfare
CF	Conventional Forces
CGS	Common Ground Station
CIA	Central Intelligence Agency
CINC	Command-in-Chief
CINC IPL	Command-in-Chief Integrated Priority List
CINCUSSOCOM	Command-in-Chief U.S. Special Operations Command
CJCS	Chief, Joint Chiefs of Staff
COE	Common Operating Environment
CONUS	Continental United States

CS	Combat Support
CSS	Combat Service Support
CSSCS	Combat Service Support Control System
CSS/EAC	Combat Service Support at Echelons Above Corps
DCSINT	Deputy Chief of Staff Intelligence
DCSS	Digital Communication Satellite Subsystem
DIA	Defense Intelligence Agency
DISE	Deployable Intelligence Support Element
DMA	Defense Mapping Agency
DoD	Department of Defense
DPG	Defense Planning Guidance
DSCS	Defense Satellite Communications System
DSN	Defense Switch Network
EAC	Echelons Above Corps
EMP	Electromagnetic Impulse
EPLRS	Enhanced Position Location Reporting System
EW	Electronic Warfare
EXFOR	Experimental Force
FAADC2I	Forward Area Air Defense Command Control and Intelligence System
FAX	Facsimile
FBCB2	Force XXI Battle Command Brigade and Below system
FCR	Future Capabilities Requirements
FLOT	Forward Line of Own Troops
FM	Field Manual

FM	Frequency Modulation (radio channel)
FOB	Forward Operating Base
FTP	File Transfer Protocol
FY	Fiscal Year
GCCS	Global Command and Control System
HF	High Frequency
HPT	High Payoff Target
HUMINT	Human Intelligence
HVT	High Value Target
IDHS	Intelligence Data Handling System
IEW	Intelligence and Electronic Warfare
IPL	Integrated Priority List
ISHMRS	Improved SOF High-Frequency Manpack Radio System
IVIS	Intervehicular Information System
JCS	Joint Chiefs of Staff
JDISS	Joint Deployable Intelligence Support System
JROC	Joint Requirements Oversight Council
JSCP	Joint Strategic Capabilities Plan
JSOTF	Joint Special Operations Task Force
JSTARS	Joint Surveillance Target Attack Radar System
JTF	Joint Task Force
JWCA	Joint Warfighting Capability Plan
JWIC	Joint Worldwide Intelligence Communications System
JWID	Joint Warrior Interoperability Demonstration

Kbps	Kilobits per second
LAN	Local Area Network
LAN/WAN	Local Area Network/Wide Area Network
LRS	Long Range Surveillance
Mbps	Megabits per second
MCS	Maneuver Control System
MG	Major General
MI	Military Intelligence
MSE	Mobile Subscriber Equipment
MSE/TPN	Mobile Subscriber Equipment/Tactical Packet Network
MSS	Mission Support Site
NAVSOF	Naval Special Operations Force
NCA	National Command Authority
NMS	National Military Strategy
OCONUS	Outside the Continental United States
OCR	Operational Capabilities Requirements (see also FCRs)
OPORD	Operations Order
OPTEMPO	Operational Tempo
PIR	Priority Intelligence Requirements
POM	Program Objective Memorandum
PSYOP	Psychological Operations
RCP	Relevant Common Picture
RD&A	Research, Development, and Acquisition
RF	Radio Frequency

RISTA	Reconnaissance, Intelligence, Surveillance, and Target Acquisition
SATCOM	Satellite Communications
SCAMP I	Single Channel Anti-Jam Manportable Terminal I (first version)
SHF	Super High Frequency
SINCGARS	Single-Channel and Airborne Radio System
SF	Special Forces
SFODA	Special Forces Operational Detachment-A
SOCRATES	Special Operations Command Research, Analysis, and Threat Evaluation System
SOCCE	Special Operation Command and Control Element
SOCOM	US Special Operations Command, also called USSOCOM
SOF	Special Operations Forces
SOF IV	SOF Intelligence Vehicle
SOFTACS	Special Operations Forces Tactical Assured Connectivity System
SR	Strategic Reconnaissance
S&T	Science and Technology
STACCS	Standard Theater Army Command and Control System
STO	Science and Technology Objectives
TAP	The Army Plan
TCP/IP	Transmission Control Protocol/Internet Protocol
TDA	Table of Distribution and Allowances
TDO	Technical Development Objectives
TENCAP	Tactical Exploitation of National Capabilities (program)
TFC	Task Force Commander
TMD	Theater Missile Defense

TRADOC	Training and Doctrine Command, also called US Army Training and Doctrine Command
TROJAN SPIRIT II	Trojan Special-Purpose Integrated Remote Intelligence Terminal II (second version)
UHF	Ultra High Frequency
USAF	US Air Force
USASOC	US Army Special Operations Command
USATRADOC	US Army Training and Doctrine Command, also called TRADOC
USSOCOM	US Special Operations Command, also called SOCOM
VHF	Very High Frequency
WAN	Wide Area Network

CHAPTER 1

INTRODUCTION

The Situation

The future of the United States Army is brighter than it has ever been, considering what technology the twenty-first century will offer. The army is involved in a complicated process of development that is spreading from top ranks and extending to the field. Through the efforts of thousands of people, the army is organizing, synchronizing, and digitizing itself into the twenty-first century. The result will be a new army with a new way of defending the nation's interests. The question is, however, are all these new systems really synchronized, organized, and digitized, and will the Force XXI concept really work? Only the future will reveal the answer. A subordinate question, and the central question of this thesis, is will special forces (SF) teams be seamlessly connected to the intelligence systems of Army conventional forces (CF) in Force XXI?

The terms, special operations forces (SOF), Army special operations forces (ARSOF), and special forces (SF), are closely related and, thus, deserve definition. SOF refers to special operations forces of all the services. The commanding headquarters is U.S. Special Operations Command (USSOCOM)(hereafter called SOCOM). ARSOF applies only to Army special operations forces and is also an overarching term, but only within the Army. The ARSOF senior headquarters is the U.S. Army Special Operations Command (USASOC). Special forces is a specific special operations force within the Army. Soldiers of the special forces are generally referred to as the green berets. The SF is part of both the ARSOF and SOF communities. The SF senior headquarters is USASOC.

Historically, the relationship between SOF and conventional forces has been troubled. The majority of the Army's force structure consists of conventional forces., which include infantry, armor, field artillery, and all the supporting forces. When the Army introduced the concept of removing soldiers from the conventional force to serve in special units, conventional force senior leaders did not like the idea of their best soldiers being removed to start an elite organization. They felt the concept was contrary to the basic paradigm of team building. The best soldiers usually became leaders. Removing the best soldiers from the team removed potential leadership, which in turn weakened the team structure.

Over time, however, special forces have become a permanent part of the Army. But old traditions and opinions die slowly. There is still a stigma connected with special operations forces, but the stigma is slowly disappearing. However, units within the SOF community, especially special forces, have supported conventional operations by providing critical human intelligence behind enemy lines to interpret the intentions of the enemy. Consequently, ARSOF and CF communities have cooperated to develop doctrine to provide directives for the necessary interoperability needed between the two forces. Also, special operations forces have worked side-by-side with conventional forces in the difficult and convoluted operations of peacekeeping and peacemaking.

Today, interoperability enables forces to conduct missions without retraining soldiers, because nomenclature and methods are similar enough for all to understand. Interconnectivity enables the forces to communicate during crisis and peace without undue time or equipment deficiencies. In the future, the realities of the interoperability and interconnectivity of special operations and conventional forces will remain primary factors in the conduct of smooth and effective operations. Field Manual (FM) 100-25, directs how special operations and conventional forces will work together.[1]

When considering the monumental task of creating the twenty-first century Army, and in light of the bumpy relationship of special operations forces and conventional forces in the past, there exists a question of whether these two forces will be able to interconnect in the future. This thesis attempts to answer a portion of that question.

The following paragraphs define some specific definitions used in this thesis. Others are in the Glossary.

The term seamless implies the connection of two entities so that they work as one entity without disconnects.

The concept of sensor-shooter linkage implies that there is a direct link between a sensor that finds and identifies enemy targets with weapons systems that destroy targets. This communications link must be nearly instantaneous between two entities.

The concept of real-time information implies that whatever link exists, the information will travel at speeds that are near instantaneous. This affords the opportunity to destroy that enemy target within seconds from identification and before it disappears from the sensor.

The last concept is the relevant common picture. This implies that all soldiers can see the same picture at their individual locations simultaneously. The decision maker can see the enemy first and within seconds and take action to destroy that enemy within seconds before he knows he has been detected.

All Army special operations forces are under the command of USASOC. For specific missions and special operations-specific equipment, ARSOF looks to SOCOM. There are several types of SOF within USASOC, but for this thesis the specific force addressed is called special forces (SF). Special forces consists of specially trained soldiers who conduct operations behind enemy lines to gather information, destroy enemy facilities, or raise and train local citizen units to do the same.

Intelligence terms requiring definition are sensor, processor, and analysis. The sensor is the entity, either human or electronic, that finds the enemy. The processor is the information system that receives, converts, and correlates raw data into a form usable as combat information or intelligence. Analysis involves the action humans perform to derive importance from processed information and what it means to the commander. The end result is the interpretation of the enemy's intent and why. Another important term is communications, which is the link to sensors, processors, and commanders.

The explanation of interconnectivity implies the result of a connected and interoperable system between two entities that affords easy movement of information back and forth. "Inter" means between or among, and "connectivity" means a logical relationship. Interoperability implies the ability of two entities to conduct a mission together without special equipment. That is, their equipment operates with other entities without modification. Thus, this thesis is an investigation of the logical relationship between Army SF and CF intelligence systems in the twenty-first century.

In past operations, such as Desert One, Grenada, and to some extent Just Cause and Desert Storm, the services experienced a lack of interconnectivity and interoperability in the areas of operations terminology, communications, and intelligence support.

> From Grenada to Panama, from the Persian Gulf to Somalia, the problems were often similar: service stovepipes and resulting inconsistent support, consistently the biggest shortcoming. Frequently information was collected in a timely manner and analyzed correctly only to get bogged down in a dissemination system that failed to serve customers.[2]

The result was the unnecessary loss of lives and equipment. Interoperability has been greatly improved by experience and by updated manuals.

During Desert Storm there was an improved sharing of intelligence information between national agencies and the Department of Defense (DoD). This was a great improvement over previous experiences, but the time lag for information still approached 12 to 24 hours. Based on these experiences, a connection between national intelligence-gathering agencies and DoD must be enhanced in order to share intelligence faster. To benefit from the improved sharing of information

between national agencies and DoD, the services, and particularly the Army, are creating twenty-first century concepts for computer-based forces.

The challenge for the future is whether the Army can become a twenty-first century force and maintain its fighting edge to remain the superpower of the world. The powerful impression created by U.S. military power during the Gulf War, the preeminence of the U.S. in a wide range of military technologies, and the frequently demonstrated competence of U.S. armed forces seem likely to deter an attack on American interests by regular armed forces in the foreseeable future. However, the U.S. position as a global leader makes it a target for those who wish to upset the international or regional status quo.

The challenges to U.S. security outlined in defense planning guidance include the proliferation of nuclear weapons; regional crises; threats to democracy; threats to the economy; and transnational threats, such as drug and crime cartels; international terrorists; and even some commercial enterprises; narcotrafficking; crime and revolutionaries; human suffering; and rising crime. All of these can lead to war. Combining the U.S. position in the world as the superpower with the threats of the twenty-first century, the likelihood is high that the U.S. government will place its armed forces in harm's way more than once. There will be many new weapons and methods with which to wage war.

The joint staff has developed the "C4I for the Warrior" concept as a joint interoperability objective. (C4I stands for command, control, communications, computers, and intelligence.) The C4I system creates a broadly connected joint system of systems that provides a common operating environment (COE) to provide total battle space information to the warrior. This concept is implemented by the Global Command and Control System (GCCS), which is intended to integrate and synchronize all governmental and DoD agencies on one compatible network. The Army's program to interface with the GCCS is the Army Battle Command System (ABCS). The desire is to

have all services share information among themselves as well as with national agencies. To continue to be the world's superpower, the U.S. must modernize the Army so it can share information instantaneously. If it cannot, it will lose its edge over enemy forces.

SOCOM does have a C4I plan oriented to planning, guiding, and providing a vision for the interoperability and interconnectivity of SOF with joint and national assets. To accomplish the revolution or evolution in military structure and action, the Army has developed a concept or vision called Force XXI. This concept is the Army's answer to the twenty-first century's threat. Force XXI's premise is that--

> Emerging information and digital technologies will create a synergistic effect among weapons, organizations, and components, significantly enhancing the Army's capabilities. Force XXI will synthesize the science of modern computer technology, the art of integrating doctrine and organization, and the optimization of the Army's quality people. The goal is to create new formations that operate at even greater performance levels in speed, space, and time. Force XXI will encompass the reconceptualization and redesign of the force at all echelons. . . It will focus on connectivity--how the Army puts the force together when it is employed. . . Decisive victory in the twenty-first century will be achieved by domination of the enemy in speed, space, and time; and by achieving and sustaining a high pace of continuous, all-weather operations. . . Force XXI will be ideally suited for joint operations. Seamless connectivity with other elements of the joint force is essential for successful future operations. Force XXI's technology will be fully compatible with the systems of other services. . . The main effort of the (Force XXI) campaign plan is to redesign the operational forces of the Army--from the foxhole to factory.[3]

This premise implies a requirement for fast and effective intelligence distribution to any friendly participant in the battle at all times. This ability to control information in battle will enable the Army to stay ahead and, therefore, surprise the enemy. To this end, the Army has developed a holistic requirements-based process for determining what equipment is necessary for warfighting in the twenty-first century. The concept is formed from a variety of input, including National Security and National Military Strategies, lessons learned from operational experiences, and future conflict scenarios. All of this is weighed against the science and technological possibilities of the twenty-first century.

This integrated approach to information-sharing is the Army's concept of "digitizing the battlefield," which requires an interneted system of computers to share information in real time from all sources. This will require a developmental path toward a more interactive computer architecture to ensure that SOF and CF are connected and able to access and share all information that will influence their missions. This requires an interconnected intelligence system that provides information gathered from all sources into a single system, available to all users. Equipment would have to be interconnective and software would have to be communal. The requirements of SOF and CF for this system would be based on each's idiosyncrasies, mission requirements, and how the forces operate.

Conventional forces operate at the operational and tactical levels of war. Therefore, conventional forces are interested in intelligence concerning the execution of battles and engagements (tactical) or the link to strategic objectives (operational). (See FM 100-5.)[4] However, conventional forces do not regularly provide intelligence except at the tactical level of war.

Conversely, special operations forces operate at the operational or strategic levels of war. They require and gather intelligence about long-range, worldwide perspectives driven by national objectives. Special operations forces provide and use intelligence. They must be interconnected with conventional forces, other services, and government agencies such as the Central Intelligence Agency (CIA), the Defense Intelligence Agency (DIA), and so on. In addition, doctrine requires special forces and conventional forces to work together; that is, be interoperable, at the senior levels of command (corps and echelons above corps (EAC)). (See also FM 100-25.)[5]

Having to act within the demands of these variant levels of war causes a disjuncture between the necessary interconnectivity of SOF and CF. This disjuncture is a major hindrance for these forces in the development of integrated communications equipment and systems.

The Purpose of This Thesis

This thesis discusses the Force XXI concept for ARSOF and CF intelligence and communications systems. The research investigates--

-- The development of the Force XXI concept.

-- The Army's development and acquisition process.

-- The communications plan for digital traffic.

-- The intelligence architecture for the twenty-first century.

Other topics provide background for an understanding of the thesis question.

The Force XXI concept can be reduced to its most relevant components--a seamless sensor-shooter linkage, real-time information, with a relevant common picture. Therefore, research was limited to Force XXI development, the interaction between SOF and CF, and the intelligence plan for Force XXI.

The development process, as it exists today, determines the communications and computer networks and equipment of tomorrow. Therefore, an analysis of the current research development and acquisition (RD&A) or the Concepts Based Requirements System (CBRS) process is at the heart of this thesis.

It is also necessary to investigate the integration of signal plans for digital communications between computers. Future equipment must ensure that the transfer of information is interconnected, timely, and synchronized with intelligence equipment.

The U.S. Signal Corps plays a vital role in the interconnectivity of intelligence systems. It will provide the necessary communications links to allow interconnectivity. A subordinate thesis question is does the Signal Corps share the vision of the twenty-first century battlefield? If so, will it have to redirect technology development to be synchronized with intelligence developments?

This thesis does not cover integration or connectivity with other services. But, it may discuss connectivity with national and joint assets when it is necessary to further explain the main thesis question. The intent is to include only information that illuminates the thesis question: Will special forces (SF) teams be seamlessly connected to the intelligence systems of Army conventional forces (CF) in Force XXI? Additional and supporting questions to the main thesis question follow--

1. Does the Force XXI concept plan to interconnect the Army with joint/national assets?
2. Are SOF and CF interconnected in the requirements process?
3. Are SOF and CF interconnected in the RD&A process?
4. Does the intelligence plan for RD&A interconnect SOF/CF?
5. Is the Army planning to interconnect ARSOF and CF in the RD&A process?
6. Is SOCOM planning to interconnect SOF/CF in the RD&A process?
7. Are national and Army intelligence interconnected in RD&A?
8. Is the intelligence architecture currently interconnected?
9. Currently, are there efforts to interconnect the intelligence architecture?
10. Currently, are there problems with the intelligence architecture?
11. Do Force XXI plans show interconnectivity and compatibility?
12. Is ARSOF/SOF planning to meet with the Army to synchronize Force XXI plans?
13. Is there a plan to integrate all parties and systems in the future?
14. Is there a matrix to ensure parallelism between ARSOF and CF?
15. Do plans address speed, size, and security?
16. Will the system being planned result in a seamless sensor-shooter link for ARSOF/CF?
17. Do plans address bandwidth?

This thesis also asks, whether special operations forces have a vision of where they are going in the twenty-first century, how they will get there, and how they will interface with the rest of the Army? Do conventional forces have a vision of the future, a plan for how to get there, and are they developing the requirements through experiments? Does the intelligence branch share the vision of other Army components, and does it have a plan of how to get there?

---

[1] U.S. Army, *Field Manual 100-25, Doctrine for Army Special Operations Forces* (Washington: Department of the Army, 1991), 2-4. Hereafter called FM 100-25.

[2] Thomas R. Wilson, *Joint Intelligence and Uphold Democracy*, Joint Force Quarterly, #7, Spring (February) 1995, pp. 54-59.

[3] U.S. Army, *United States Army Posture Statement FY96* (Washington: Department of the Army, 1995) February 1995, 52-54.

[4] U.S. Army, *FM 100-5, Operations* (Washington: Department of the Army, 1993), 6-2,6-3.

[5] *FM 100-25*, 4-36.

CHAPTER 2

REVIEW OF LITERATURE

There are volumes of written material that provide background knowledge of the topic of this thesis. However, there are no works that specifically address the interconnectivity of intelligence for SOF and conventional forces in the twenty-first century (Force XXI). The background material is in many locations and media. The Internet contains home pages on Force XXI, Intelligence XXI, the acquisition web, U.S. Army Training and Doctrine Command (USATRADOC) (hereafter called TRADOC) pamphlets, the Army Concepts Based Requirements System (CBRS) process, the Army Digitization Office Master Plan, and the Signal School's C4I plan. There are also Army battle lab results, TRADOC operational capabilities requirements (OCRs), the Army Science and Technology Master Plan (ASTMP), and articles written by General Gordon R. Sullivan (former Vice Chief of Staff) and others on Force XXI. Periodicals, such as the *Army Times*, *Army* magazine, *Military Review*, the *Joint Force Quarterly*, and the *Armed Forces Journal* all contain articles on Force XXI. There are also a few monographs that address background topics that add to the knowledge base. The two most applicable are a monograph that addresses SOCOM's RD&A process and one that addresses the command and control (C2) system for Force XXI. There are also a number of general officers who have observed experiments and provided input for Force XXI concept development.

The crucial information for this thesis was produced by the Intelligence School and USASOC. These are the two most important entities concerning the intelligence interconnectivity of ARSOF and Army conventional forces. The commanders and staff officers of these headquarters will determine the future of intelligence interconnectivity.

This thesis identifies disconnects in Force XXI planning for ARSOF and Army conventional forces. If the Army is to fight as a single, synchronized unit, it must seamlessly link sensors with shooters and establish a relevant common picture in real time by planning, researching, acquiring, testing, and performing in the field as one entity. There is no information that addresses the interconnectivity of ARSOF with conventional forces, much less the interconnectivity of intelligence systems.

There are many opportunities for further research in this field. The relevant common picture and seamless sensor-shooter link require a common map reference among all computers and a minimum resolution for accuracy. There are also many issues to be resolved whether the Force XXI concept is conceivable from the map viewpoint.

Another area of research is in communications networks and their capabilities to handle the amount of traffic that occurs between command headquarters during a battle. For instance, how much bandwidth is needed for C2, intelligence, fires, and CSS to communicate and to provide a relevant common picture in real time with seamless sensor-shooter linkage? When should it be available?

Still another area of interest is the divergent focus that USASOC must take for future development between the joint and national direction that focuses SOCOMs on the strategic and operational levels of war versus the more "enemy-focused" operational and tactical levels of war. The divergent focuses causes a conflict in establishing intelligence interconnectivity. Another area of research concerns what ARSOF provides the Army versus what SOCOM provides. For example, are SOF missions congruent with these two differently focused headquarters?

The final area of interest is to determine where the weak links in the Force XXI system are that a computer hacker enemy could attack. This is where the enemy could introduce computer viruses or misinformation to destroy or disable our information systems. However, the Force XXI

system, must be able to interface with worldwide systems somehow, somewhere, to remain abreast of the world situation.

One of the criteria for determining if the research is valid and focused is the qualifications of the researcher. The researcher has been a member of the SOF community for ten years and has commanded a SF team and company, in addition to a conventional force company. He has served on USASOC staff when it was called 1st SOCOM and just recently returned from Panama after serving with the Special Operations Command South. He has been involved in exercises and missions that required interfacing with other services and nations. Foremost, he has experienced a lack of interconnectivity which had to be overcome in order to yield a synchronized and interoperative headquarters.

CHAPTER 3

RESEARCH METHODOLOGY

The research plan for this thesis follows a general-to-specific methodology to help the reader understand the background information that prepares a setting for the subject. While the methodology proceeds from general to specific, it also answers pertinent research questions. The intent is to educate and focus the reader while moving toward a conclusion. The reason for this thesis was to investigate whether what is planned for Force XXI will lead to what can be expected to occur in the future.

To gain a general idea of the history of the concept, the author conducted research on the origins of Force XXI. Force XXI began as an idea General Don Morelli generated during a meeting with Alvin and Heidi Toeffler, the authors of *Future Shock*.[1] The idea was the postulation of a computerized information-based Army. This idea was nurtured to create a comprehensive, dedicated, and evaluated program of digitizing the battlefield. The Toefflers further defined and updated this future battlefield in their book *War and Anti-War*.[2] The Army's Force XXI concept and all of its components are a visualization of the future battlefield and what the Army will be capable of doing beyond the year 2021.

To gain an understanding of the Force XXI development process, the author looked at the concept's components and interconnections. When developing the concept, the Army produced a set of goals called Army modernization objectives (AMOs). The Army also established five battle labs that would have functional responsibilities based on each of five battlefield concepts known as battlefield dynamics. The labs were to be think tanks for developing the force for the twenty-first

century. Combining the AMOs, battle labs, and Force XXI concepts yielded the need for operational capability requirements (OCRs). Planners write one set of OCRs for each of the five battlefield dynamics and give them to a battle lab to develop. The battle labs tested and assessed the concepts that were to make the OCR become reality. The labs were also responsible for branch contributions Army wide for each OCR.

The Army initiated a number of panels, offices, experiments, and boards that empowered specific branches of the Army to conduct particular portions of Force XXI development. One of the offices, the Army Digitization Office (ADO), was created to ensure the total integration of all branches with national agencies. The ADO was to outline, monitor, evaluate, and correct the actions of all other entities working on the computer and communications side of Force XXI. The outline became the Army Digitization Plan (ADP), which focuses and provides a vision for the different agencies and branches of the Army. As an adjunct to the ADP, the Army instituted the Army Science and Technology Master Program (ASTMP) to provide a warfighting focus to the U.S. technology base.

Currently, the Force XXI concept is being researched in a field environment by an experimental force (EXFOR) at Fort Hood, Texas. The EXFOR is using existing hardware to test Force XXI ideas and to provide feedback on the feasibility of and requirements for achieving the Force XXI vision.

The thesis also investigates the proposed intelligence plan for Force XXI. To develop a more in-depth understanding of this portion of the research, the questions asked were, does the intelligence Force XXI plan provide for the implementation of interconnectivity between ARSOF and CF? And, does the plan include providing an interface between national agencies, ARSOF, and CF?

The author next examined data to find out if SOF and CF are working together in the requirements process and if they are interconnected. Other questions are: Does the Army include

SOF in its Force XXI requirements process? Does SOF participate in the Army RD&A process? Is the intelligence process for Force XXI interconnecting SOF and CF? Is the USASOC a member of the development process at all levels to ensure interconnectivity with conventional forces and national agencies? Is the development process synchronized? And finally, is communications equipment development synchronized with the Force XXI intelligence process?

The author then determined whether the intelligence branch is including the interconnectivity issue for ARSOF and CF as part of the overall plan. Is the intelligence architecture, equipment, and software development for Force XXI synchronized between SOF and CF? Do USASOC and the Army plan to meet to establish a focus for the intelligence system? Do USASOC and Army CF meet to ensure focus is maintained? Is there a matrix that ensures a parallel and synchronized development? Do future plans show equipment, software, architecture, and communications interconnectivity and compatibility? Do future plans address speed, size, and security with interconnectivity?

The research was comprehensive and covered all pertinent issues. The importance of establishing a thorough background was of utmost importance to enable the reader to fully understand the many areas of concern that affect the thesis subject. The background information mostly concerns the interface that existed between the Army and ARSOF at the requirements stage. Theoretically, ARSOF and CF, as planned, will have an interconnectivity.

---

[1]Alvin and Heidi Toeffler, *Future Shock* (New York: Bantam Books, 1970) 561.

[2]Alvin and Heidi Toeffler, *War and Anti-War* (New York: Warner Books,1995) 302.

CHAPTER 4

ANALYSIS

The purpose of this chapter is to lead the reader through the mounds of research information to focus thought and refamiliarize the reader with the central thesis question: Will special forces (SF) teams to be seamlessly connected to the intelligence systems of Army conventional forces (CF) in Force XXI? Throughout the chapter there are passages that specifically address each question this thesis asks.

The Challenge

According to the Defense Planning Guidance (DPG) extracted from the National Military Strategy, the challenges to future U.S. security are--

> the proliferation of nuclear weapons, regional crises, threats to democracy and the economy, transnational threats such as drug and crime cartels, international terrorists and even some commercial enterprises, narcotrafficking, crime and revolutionaries, human suffering, and rising crime.[1]

Because the majority of these threats to future world peace appear to not be from regular armed forces, the U.S. must look hard at its capabilities and methods to counter such threats. The position of the U.S. as a global leader makes it an obstacle to those who wish to upset the international or regional status quo. However, the powerful impression the U.S. military created during the Gulf War, the preeminence of the U.S. in a wide range of military technologies, and the frequently demonstrated competence of U.S. armed forces seem likely to deter an attack on American interests by regular armed forces in the foreseeable future.

The Future Threats

According to Alvin and Heidi Toeffler in their popular book *Future Shock*, the twenty-first century's basis of economic strength (agrarian, industrial, and information-based) will operate at three sharply different clock-speeds corresponding to the level of sophistication of each nation.[2] These differences will fuel the conflicts of the twenty-first century.

The Toefflers see the world as being divided into two rival factions: a high-tech "have" faction that controls a large amount of the world's information and leads the way in everyday business, economics, diplomacy, and probably military might. The other part of the world contains the "have nots" or needy faction that follow rather than lead and who take what they can get to survive in business, economics, and even food. The haves will reside in North America, Europe and the economically successful nations of the Pacific rim. The have nots will occupy the rest of the world, living in chaos, with passions fueled by radical religious fundamentalism, ethnic hatreds, disease, exploding populations, declining natural resources, and pervasive crime that challenges the very foundations of national states. These have nots will have no regard for borders and some will even reject, or vilify, Western ideas of progress, rights, duties, and responsibilities.

This widening gap is evident in the current space race, where the split between space powers (haves) and non-space powers (have-nots) is growing. The future effect could be devastating because of the expanding use of space for military and everyday endeavors.

The difficult part of this new age will be to manage the increasing amounts of information and the associated complexity. It will require new forms of leadership, fast thinking, decision making, and an extremely high order of systemic integration. This new information age will be an era when controlling information will equate to controlling knowledge, and in turn, knowledge will control world enterprises. The concept is that the appropriate data, information, and/or knowledge will reduce

the need for other input. For example, a computer-driven cutting tool will reduce the need for personnel and supplementary materials or machines, thereby using fewer materials and resources.

This same scenario can be projected for an information-based future army. The future soldier will have truly space-age capabilities with information dominance being the base feature. This, in turn, will change the parameters of range, lethality, and speed of action. The Toefflers call the soldier of the future a "Ph.D. with a Rucksack."[3] The sophisticated equipment he will use and knowledge he must acquire will force him to study, be quick of mind, and have a wider view of his world.

Future Technology

The equipment available to the soldier of the future will span the gamut from chameleonic camouflage to biomechanical suits to liquid embrittlement compounds. Future wars could even be waged with genetically engineered material ranging from the use of microbes, androids, biocomputers or highly miniaturized weapons. Capabilities include--

-- Bioengineering super plagues that are engineered to kill only certain ethnic groups or to breed parahumans to do a nation's fighting.

-- Methods to trigger earthquakes or volcanic eruptions at a distance by generating certain electromagnetic waves.

-- Modifying the weather to deflect wind currents in order to disperse genetically altered insects to devastate a selected crop.

-- Using lasers to cut a custom-tailored hole in the ozone layer over an adversary's land.

-- Nonlethal methods of dealing with crowds using infrasound generators that emit very low frequency sound waves to cause temporary disorientation, nausea, and loss of bowel control.

-- Using the media to influence the emotions, motives, objective reasoning, and ultimately, the behavior of people.

-- Using smart armor on tanks to sense an incoming projectile's approach.

-- Paralyzing tanks, armored personnel carriers, and trucks through the use of special munitions that temporarily contaminate fuel or change its viscosity to degrade engine function.

-- Using directed-energy weapons to change the molecular structure of targets, to keep planes on the ground, or to make bridges unstable.

Future Operations Vignette

The following vignette provides a glimpse of a future special operations team and its possible capabilities in the twenty-first century and beyond.

A team of soldiers has the mission to retarget the enemy's missiles and plant some weapons, if the enemy does not cease its warlike ways. While the team prepares for the mission, it is protected by a group of intercommunicating robotic vehicles that are programmed to determine friend from foe and destroy intruders.

The team trains for the mission using 3-D holographic equipment that simulates the threat. This enables the commander to execute the plan with a fighting enemy in virtual reality and make the necessary changes to prevent death or injury on the actual mission.

Space satellites will have provided extremely fine-grained photos, radar images of foreign territory, and electronic map overviews locating enemy ships. The satellites will have listened in and transmitted information gathered from foreign electronic transmissions about the intent of the enemy concerning the current crisis.

Smart mines will have been planted around the team's infiltration site to acoustically scan the area, compare engine sounds and earth rumbles against a list of vehicle types, identify the target, use an infrared sensor to locate it, and then destroy an enemy vehicle by firing a shaped charge. The team would then infiltrate the mission area--on this occasion by aircraft. The aircraft can fly horizontally for 1,000 nautical miles then transition to vertical flight to allow quick and safe exit. During the flight, the team continuously rehearses the mission in virtual reality.

To increase efficiency on the ground the team will use high-technology equipment such as filmless electronic cameras, lightweight portable power units, automatic voice-translating equipment with a dial-in language selector, and lightweight rugged radios that combine a global positioning unit, fax, and on-line coding/decoding capability with a low probability of interception or detection.

Team members wear a chameleonic camouflage suit, which changes as needed depending on the surroundings and which offers protection against nuclear, chemical, or biological weapons. The suit also contains night-vision goggles, a heads-up display that provides a relevant common picture of the battlefield, and an aiming system that tracks eye movements and automatically points a weapon to where the soldier is looking. The suit is also an intelligent exoskeleton that learns to perform the soldier's repetitive tasks and amplifies his strength several fold.

While the team moves to the mission site, unmanned patrol boats launch multi-legged robotic devices to plant mines or sensors. These robotics can infiltrate in otherwise inaccessible places, to gain control of in-bound shipping destined for the enemy, for example.

Once the team gains entrance to an office building (one of the enemy's computer centers), it implaces devices that will lie dormant until remotely activated. In preparation for an attack, the devices will destroy the communications system by burrowing into the communications wires. The team uses their computer to spoof the enemy's computers by sending false signals, and implanting messages to alter records and to gain access to the enemy's weapons guidance systems. The team can then alter guidance systems to disarm, arm, or retarget the weapons.

On the way out of the office, a team member might open a small box of robotic reproductive ants, which can infest the building and slowly destroy the enemy's communications system. As team members move out of and away from the building they strategically place a few super-smart nanometer-size sensor mines that can reproduce themselves within the hour and remain undetected and harmless until the team, from a distance, selectively arms them.

While making their way to the exfiltration site, the team uses one of the laser rifles to damage some enemy optical and infrared equipment on the outskirts of the city. They are also prepared to use the laser rifles to cause temporary flash-blindness on any enemy civilians who happen to notice them.

To prevent the team from being followed, one of the team members distributes antitraction agents to make surrounding surfaces slippery, thereby limiting use of the area. Team members notice some vehicles close to the exfiltration site and decide to further protect their exit by applying polymer adhesives on the ground to glue the equipment in place. When they reach the exfiltration site, they notice an enemy soldier on guard duty near the site. A member of the team sneaks up to a position close enough to use a calmative agent that induces sleep.

As the aircraft is retrieving the team, a few enemy soldiers notice the aircraft and run toward the area. As the enemy soldiers slip on friction-reducing agents laid down by the team, the team kills the intruders. However, one team member has been wounded. On the flight back to friendly lines, the medical specialist implants nano-robots that are small enough to operate like submarines in the bloodstream of humans to perform surgery at the molecular level to save the soldier's life.

This vignette might sound far-fetched, but by extrapolation of the current explosion of technological development into the next century assures us that many of these possibilities can become reality.

Force XXI Concept

General Don A. Starry, contemplating the 1973 Arab-Israeli War, observed the simple fact that "starting ratios do not determine the outcome. Whoever seizes the initiative, whether he is outnumbered or outnumbering, whether he is attacking or defending, will win."[4] Delaying and disrupting the enemy deep in the battle area stops the orderly advance of the enemy's follow-on echelons and the army's advance. The Israelis used the age-old practice of attacking from an unexpected direction instead of attacking the main point of Syrian strength. Seeing this old practice

in a new light caused Starry to formulate thoughts of how to enable an Army to effect this kind of action against any enemy. As a result of his observations, General Starry began a campaign to change the Army's way of thinking. He directed a fellow general officer, General Don Morelli, to start the process.

On 12 April 1982, in Washington, D.C., General Morelli met with authors/futurists Alvin and Heidi Toeffler. They discussed the future of the U.S. Army, calling the new era the "Information Age," which became a reality during the Gulf War. The Information Age is defined by the parameters of--

-- Destroying the enemy's command facilities.

-- Destroying communications to prevent information from flowing up or down the chain of command.

-- Taking the initiative, striking deep, and preventing the enemy's backup echelons from going into action.

-- Integrating air, land, and sea operations.

-- Synchronizing combined operations.

-- Avoiding frontal attack against the adversary's strong points.

-- Knowing what the enemy is doing before he does it while concealing friendly actions.

In the 1990s, General Gordon R. Sullivan, Chief of Staff of the Army, characterized Information age warfare by identifying five trends--

> greater lethality and dispersion, increased volume and precision of fire, better integrative technology leading to increased efficiency and effectiveness, increasing ability of smaller units to create decisive results, and greater invisibility and increased detectability.[5]

Following Desert Storm, General Gordon R. Sullivan and General Frederick Franks, TRADOC Commander, faced a Congressional directive to downsize the Army. Realizing the impact of this directive, they brainstormed how to become smaller while preserving the existing warfighting

potential. They decided the only pragmatic way to achieve their goal, and remain the dominant land combat force in the world, was to exploit the emerging technologies of the information age.

> Given the fact that we would be stuck with our existing fleet of combat systems for years to come, information age technology offered the most feasible and affordable means of preserving combat dominance as we became the world's eighth-largest army.[6]

These visionary leaders observed that the power of the information age offered a capability to dramatically enhance the combat potential of the combined arms team while dominating the battlefield through knowledge. They could achieve this principally through the creation of accurate situational awareness (either friendly or enemy), rapid and accurate target locating, and total asset visibility across the spectrum of CSS operations. They also believed that enhancements to the Army's war fighting ability through the power of knowledge would occur principally in the areas of lethality, survivability, the operational tempo (OPTEMPO) of battle, and force protection--the components of victory in any fight.

> In simple terms, the potential exists to kill more enemy targets faster by massing combat power more effectively and precisely, to control the operational tempo of the battle, thereby retaining the initiative, and to lose fewer soldiers.[7]

The result is the attempt to do what commanders have endeavored to do on battlefields for at least 25 centuries: see the terrain, see the enemy, see ourselves, and visualize how to employ forces to accomplish the mission--all critical cognitive abilities based on knowledge. With the realization of this vision, munitions can be accurately emplaced to disrupt and delay the movement of enemy forces, in effect controlling the tempo of battle. The senior leadership of the Army also realized that this system must be an interoperable system that would span the services and even allied countries to allow for effective joint and coalition operations.

> Our focus for the future--Force XXI operations--must include organizations and leaders empowered to design and develop a rapidly expansible, strategically deployable and effectively employable force capable of achieving decisive results in war and operations other than war as a joint or multinational team.[8]

The goal of the future is to wield military power across space and time with heretofore unimaginable precision and accuracy. This means that there is a requirement to integrate the entire force's capabilities to resemble the effects of a single weapon. To do so, we must strive for an unprecedented ability to synchronize multiple capabilities of multiple services in time, space, and direction. Digitization or computerization of the battlefield will enable commanders to link sensors, with strike and protection means, into a protected and sustainable seamless entity whose elements are able to interact with each other effortlessly to deliver devastatingly accurate effects. The greater the capability to sense and deliver as one entity, the greater the effectiveness against the enemy.

In order to yield power, a force must obtain information. The gathering of information is the function of sensors. It is said that power, in the twenty-first century, will be derived from the ability of a force to sense the enemy, itself, and its environment; strike an opponent decisively; protect itself from the attacks of the opponent; move freely in the area of operations; exercise control over sub-elements; and sustain itself. Consequently, sensors become a primary component of information age warfare. Sensor elements could take the form of SF special reconnaissance teams, aerial reconnaissance, or any number of means designed to give the commander the capability to sense the environment.

In considering the above information, the Army developed a set of six principles for Force XXI that provide a blueprint:

1. Project the force by putting the Army abroad quickly, using pre-positioned equipment that is lighter, more durable and multipurpose, reducing lift and logistics requirements while creating the impression that the Army is an unstoppable force of unequaled competence.

2. Protect the force by using intelligence, missile defense, sensors and new technologies to make sure the Army has full control of the land battle space so the force is free to deploy, maneuver, and engage the enemy while defending itself and its facilities.

3. Shape the battle space using all combat multipliers, including feints, demonstrations, limited attack, C2 warfare, mobility, deception and available precision weapons to achieve simultaneity, thus overwhelming the enemy.

4. Conduct decisive operations using unprecedented battlefield awareness to exercise direct, continuing, and comprehensive control over land, its resources, and its people.

5. Sustain the force using focused logistics, information technology, flexible and agile CSS organizations, and new doctrine to provide rapid crisis response, delivering precisely tailored logistics packages to each level of military operations.

6. Gain information dominance by using information operations, both offensive and defensive, high-tech information systems; and sensors to make sure the Army knows more about its battle space and operations than the enemy knows about his.

The Army's intent for this information-intensive warfare is to deliberately design the force to control (maintain, accelerate, or moderate as necessary) the pace of battlefield events. In other words, combat operations should take place over the shortest feasible time at the least cost to friendly forces, enemy forces, and neutrals. To do so, Force XXI must engender the following characteristics: doctrinal flexibility; strategic mobility; tailorability and modularity; and joint, multinational, and interagency connectivity.

The Force XXI concept can be summed up by saying that--

> Emerging information and digital technologies will create a synergistic effect among weapons, organizations, and components, significantly enhancing the Army's capabilities. Force XXI will synthesize the science of modern computer technology, the art of integrating doctrine and organization, and the optimization of the Army's quality people. The goal is to create new formations that operate at even greater performance levels in speed, space, and time. Force XXI will encompass the reconceptualization and redesign of the force at all echelons. It will focus on connectivity--how the Army puts the force together when it is employed. Decisive victory in the Twenty-First Century will be achieved by domination of the enemy in speed, space, and time; and by achieving and sustaining a high pace of continuous, all-weather operations. Force XXI will be ideally suited for joint operations. Seamless connectivity with other elements of the joint force is essential for successful future operations. Force XXI's technology will be fully compatible with the

systems of other services. The main effort of the (Force XXI) campaign plan is to redesign the operational forces of the Army--from the foxhole to factory. [9]

Conceptually, real-time force synchronization will multiply combat power. Digitization ensures that the common picture viewed by the front-line unit is shared by CS and CSS elements. Furthermore, that picture will be instantaneously transmitted without error. An enemy convoy sensed by the friendly infantry unit will immediately be displayed in the supporting artillery's operations center. The combination of instantaneous communication and grid accuracy will result in rapid target servicing. Fire- for-effect will occur significantly faster with the use of smart munitions tied to an accurate grid, and no adjustment will be needed. Connectivity from the strategic level to the individual soldier is the long-term objective.

> Shared situational awareness, coupled with the ability to conduct continuous operations, will allow information age armies to observe, decide, and act faster, more correctly, and more precisely than their enemies.[10]

Perhaps Force XXI's biggest benefit to soldiers and their leaders will be in situational awareness-- the ability to know not only your own battlefield location but that of all other friendly and enemy units. For battalion, brigade, and division commanders, the synergy of combining instant information from all friendly sources--from such airborne intelligence assets as unmanned aerial vehicles (UAV) to individual tanks on the forward line of own troops (FLOT)--has great potential.

Using a tactical internet to send operations orders (OPORD) and graphics down to subordinate units at the touch of a button and to link sensor systems that locate targets with shooter systems to destroy them should allow friendly commanders to make and execute tactical decisions faster than their adversaries. Army officials call this "getting inside the enemy's decision cycle."

> The most profound implication of the new era often goes unremarked: namely, that the basic rationale for defense planning has shifted from threat to capability and from liability to opportunity.[11]

The four basic subconcepts of the Force XXI concept are seamless sensor-shooter linkage, real-time information, relevant common picture, and information dominance. Three of these (seamless sensor-

shooter linkage, real-time information, and relevant common picture) directly relate to and provide a basis for analysis and synthesis from which to arrive at a quality conclusion. Information dominance is in a sense the result of accomplishing the other three.

The seamless sensor-shooter linkage subconcept implies that there is a direct link between the sensor that finds and identifies the enemy the force is to destroy with the weapons systems that can in fact destroy the target. The subconcept of real-time information implies that which ever link exists, the speed at which the information travels from the sensor or identifying unit to the weapons system or decision maker is within seconds, thereby offering the opportunity to destroy that enemy target within seconds from identification. The relevant common picture subconcept implies that all decision makers and soldiers can see the same picture at their individual locations. This affords weapons systems commanders the ability to see the target at the same time as maneuver commanders. In its fullest sense, the Force XXI concept and its subconcepts would require complete interoperability and interconnectivity of all army, joint, and national assets and the ability to access intelligence data from all sources.

The Design of Force XXI

TRADOC is responsible for defining the Force XXI concept in the form of actionable statements that guide research and development. TRADOC Pamphlet 525-5 identifies five core principles to direct the development of Force XXI.[12] They are called battlefield dynamics and consist of battle command, battle space, depth and simultaneous attack, early entry survivability and lethality, and combat service support.

The *battle command* system will employ broadcast battlefield information integrated into a digitized image that can be displayed graphically in mobile and heads-up displays. This system will allow commanders at every level to share a relevant common picture of the battlefield scaled to each's level of interest and tailored to special needs.

> Battle command must invigorate the synthesis of information for the commander--not support more analysis for the staff to overload the commander with.[13] [SIC]

Battle space involves the ability to visualize the area of operations and the way forces interact, whether in combat or in humanitarian relief missions. Battle space may also be shaped by political constraints or other situationally unique factors. In the physical sense, battle space is determined by the maximum capabilities of a unit to acquire and engage the enemy capabilities. This will be greatly expanded by future technology. Information operations influence battle space by providing the commander the means necessary to better visualize the battle space while blinding or shaping an opposing commander's vision. Battle space then becomes a function of the commander's ability to use information that the command system provides and to employ warfighting systems to achieve the necessary balance to ensure success.

Combining the concepts of *depth and simultaneous attack*, using both lethal and nonlethal means, creates a battlefield dynamic that extends the battlefield in space, time, and purpose. (In this case, depth and deep operations are synonymous.) This combination results in reducing, if not entirely eliminating, the time and need for shaping the battlefield. It facilitates a full-dimensional attack of any enemy's center of gravity to accelerate his defeat.

The purpose of *early-entry survivability and lethality operations*, which forces tailored to create the best possible capabilities-based force conduct, is to quickly end the crisis or set the stage for follow-on forces. Based on multispectral imagery, accurate weather reports, and current intelligence information, future soldiers will be able to use simulations to repeatedly rehearse operations before performing them.

Combat service support operations will be enhanced by the future logistic system. The logistics system will link combat, CS, and CSS leaders horizontally by common information. They will then be able to visualize how they will execute an operation in harmony. An effective sustainment operation, primarily an Army responsibility, will establish the conditions for operational success.

Required Capabilities For Force XXI

To verbally establish a vision for the required capabilities of Force XXI, TRADOC wrote Pamphlet 525-66.[14] The pamphlet describes the future capability requirements (FCR), previously known as OCRs, and the battle labs program. The FCRs have been referred to as the revolution, and the path to attainment of Force XXI is the evolution.

The FCRs are derived from historical lessons learned from operational experiences, opportunities provided from the exploitation of technology, and requirements stated in the five commander-in-chiefs' (CINC's) integrated priority lists (IPL). The objective of the FCRs is to focus the battle labs and the Army science and technology (S&T) community toward capabilities that will produce Force XXI and the technological superiority needed over any potential adversary.

The Army created six battle labs, each with a vision described by each of the six battle dynamics and their associated FCRs. The battle labs conduct holistic reviews of the battle dynamic FCRs within the spectrum of Army functions: doctrine, training, leader development, organization, materiel, and soldier systems. They interact with both the Army's and industry's science, technology, research, and development community to identify technology with the greatest warfighting potential, to conduct experimentation to gain insights, and to provide an empirical basis for investment decisions.

Of primary importance is the Fort Huachuca, Arizona, Battle Command Battle Lab (BCBL) FCRs. They optimize the commander's access to and use of intelligence information, including theater and national resources (push-pull intelligence); optimize methods to broadcast intelligence of the enemy situation to the commander at each level while on the move (relevant common picture); and improve exchange of information in joint and coalition forces as it applies to intelligence and electronic warfare (IEW), information engagement, and command and control warfare (C2W). The EXFOR at Fort Hood, Texas, executes experiments in a field environment. These advanced warfighting experiments (AWE)

enable technical hardware manufacturers and computer system analysts to manipulate systems to effect the desired interoperability that Force XXI will need.

The Battle Lab Science and Technology Review is conducted annually to assess the potential contributions of individual Army science and technology projects. The total program is assessed according to FCR requirements to determine potential shortfalls, opportunities, and candidates for Army science and technology objectives (STOs). The Army Science and Technology Master Plan (ASTMP) uses FCRs to provide a warfighting focus to the technology base, funding, and in the Army STO process as a yardstick of warfighting merit.

The Advanced Concepts and Technology II (ACT II) Program provides funding and access for industry participation in the battle lab process. Topics selected by battle labs from the FCRs are submitted to the industrial community for development of advanced technologies, prototypes, and non-developmental items. These technologies can be used to enhance the battlefield dynamics previously discussed.

Battle Command

Battle command is a synergism of technologies used to increase survivability, lethality, and operational tempo. The heart of this dynamic is the battle commander, who must possess the intuitive and experiential knowledge to use the technological capabilities to their maximum extent while creating a synergy of assets to overcome the enemy. The following paragraphs describe the FCRs of interest within this battle dynamic.

Battle Command 01: Sensors. Commanders need timely and accurate sensor information about forces throughout the depth of the battle space. This information must provide a meaningful picture of the fluid and dynamic battlefield. All ground, air, sea, and space sensors must be linked into an integrated system with reprogrammable filters in order to satisfy the commander's needs at all echelons for situational awareness across the operational continuum.

Battle Command 06: Seamless, Secure, Global Information Architecture. The seamless, secure, global information architecture, which all battlefield functional areas require, must support integrated combat operations with focus on the mobile warfighting commander. The information architecture must--

-- Provide horizontal and vertical integration of voice, data graphics, imagery, and video information.

-- Facilitate operations planning, information collection, and information dissemination.

-- Enhance the commander's ability to acquire information from sensor systems, battlefield functional area systems, and from subordinate, adjacent, and higher organizations.

-- Support both analog and digital capabilities.

-- Integrate commercial and tactical communications network.

-- Provide a capability to transfer information within the architecture without requiring specific knowledge of the mechanism or platform characteristics that make up communications and automated hardware.

Implied are requirements for streamlined communications procedures and for global connectivity of extended-range communications assets. Also implied are integrated communications between the various interagency, joint, combined, and coalition forces, which include the National Command Authorities (NCA) (the President and the Secretary of Defense), operations (C2), intelligence, logistics, administrative functions, and the numerous potential echelons of a force-projection task force. Ideally, the adaptive nature of the information architecture should reduce or eliminate degradation factors that weather, terrain, distances, obstacles, electromagnetic pulse (EMP), jamming between sender and receiver, or supporting communications nodes might cause.

Battle Command 07: Interoperability. Forces require total, uninterrupted, interoperable communications. Communications should have the capability to pass between interagency, joint, and

combined forces and throughout the length and breadth of the battlefield, from the NCA level to, at times, the platoon level.

Battle Command 08: Real Time Network Management. Communications and automation capabilities are increasing, and there is a corresponding increase in the complexity of network and C4I management. A robust, adaptive, real-time C4I network management capability is required to ensure interoperability between C4I systems.

Battle Command 13: Relevant Common Picture. Situational awareness is included within the relevant common picture, which helps the commander operate within the enemy's decision cycle by allowing synchronization of forces and dictating the OPTEMPO. The relevant common picture includes timely, accurate, and relevant friendly and enemy situation information laid over a common map background with status information. Real-time situational awareness across the battlefield provides the commander with a picture of the friendly and enemy situations and reduces battlefield uncertainty by displaying the enemy's known force locations and status. The relevant common picture should also include weather and terrain products and situational updates in textual and graphic formats. Position, situation, and status information must reside on, or be available from, common data bases. The relevant common picture must be tailorable to appropriate levels of command, based on variable user-determined parameters, and be sent to multiple locations, both horizontally and vertically.

Battle Space

Battle Space (Dismounted)

The parameter, "win the reconnaissance--counter reconnaissance battle," defines the dismounted battle-space dynamic. Using reconnaissance, intelligence, surveillance, and target acquisition (RISTA) sensors (human and electronic) and unmanned vehicles protects the force and enhances firepower and maneuver. Fusion of relevant tactical data from soldier-level sensors through national assets permits leaders, from fire-team leaders through brigade leaders, an overmatch in understanding battlefield

dimensions. This will significantly enhance the dismounted force's survivability, lethality, and decisive capabilities. The following paragraphs list the applicable FCRs of this dynamic.

Dismounted Battle Space 13: Integrated Target Acquisition. This capability is key to massing effects of fires without massing friendly forces. It is required in order to provide vertical and horizontal, near-real-time, target-acquisition information throughout the task force.

Dismounted Battle Space 15: Sensor-to-Shooter Linkages. The task force commander (TFC) must have the ability to plan and control the sensor-to-shooter linkages to effectively extend his battle space.

Dismounted Battle Space 17: Increased Control of Battle Tempo. Battle command systems are necessary for providing horizontal and vertical C^2 capability in near-real time, enabling dismounted forces to operate at a faster tempo than the enemy. The systems must have the capability to gather, analyze, and disseminate information on both friendly and enemy forces from multiple sources.

Battle Space (Mounted)

The dynamic characteristics of the mounted battle space are encompassed in the commander's ability to see the battlefield. The future spectrum of intelligence-gathering tools, from global to tactical assets, will provide a clearer picture of the battlefield than ever before. The challenge is to develop technology and procedures that will ensure the ground commander receives analyzed and timely intelligence. The FCRs of interest are in the paragraphs that follow.

Mounted Battle Space 06: Intelligence for Mounted Forces. Mounted forces require the capability to access the full spectrum of intelligence information. This includes the capability to collect, analyze, produce, and disseminate timely intelligence data.

Mounted Battle Space 18: Mounted Communications and Automation. Mounted forces require the creation of reliable, redundant, horizontally integrated command and communications measures. Leaders must have a lean but functional battle command system that provides intelligence information and a view of the battlefield to enable leaders to shape their vision. New communications systems must

be secure, reliable, compatible, reduce planning time, use automated processing, and be capable of rapidly disseminating critical information and orders.

Mounted Battle Space 19: Digitization of the Mounted Force. Horizontal integration of the battlefield must be expanded through the digitization of information. Digitizing the battlefield will allow leaders to gain critical information and analyze, synchronize, integrate, and employ all warfighting systems. It is imperative that software and hardware be created that is flexible enough to rapidly respond to change as well as to meet the needs of various users.

Depth and Simultaneous Attack

The deep operations and simultaneous attack dynamic is the application of joint and combined combat power against an enemy throughout the depth of the theater of operations. The objective of simultaneous attack in depth is to accelerate the enemy's disorganization, disintegration, and destruction to create favorable force ratios long before any direct-fire engagement. To create a single extended battlefield, targeting information from all available sources must be almost instantaneously linked to a relevant common picture and decision-making process that executes fires using all accessible delivery means. Considering the joint nature of deep operations, commonality of standards and protocols incorporated into future technology becomes a key issue. The following paragraphs list the dynamic FCR of depth and simultaneous attack.

Depth and Simultaneous Attack 09: Real-Time Location and Identification of Targets. Deep attack systems must have real-time sensor data that provides sufficient detail in locating and identifying targets, reducing time lines by eliminating man-in-the-loop analysis, and improving overall responsiveness in joint precision strike and theater missile defense (TMD).

Depth and Simultaneous Attack 10: Real-Time Seamless National Targeting Dissemination. Limited connectivity and data base management exists among national sources, corps, and EAC. Future capabilities must provide real-time collection of targeting data from national sources tied directly to corps

and EAC intelligence-collection centers with the capability of linking specified shooter elements into a seamless national targeting dissemination system. This will facilitate the improved attack capability for critical targets, including missile logistic sites, infrastructure, and other key targets such as C2, follow-on forces, and targets normally associated with precision strike requirements.

Depth and Simultaneous Attack 17: Information Fusion Technology Supporting Precision Strike. Fusion of intelligence information and deep attack coordination and planning is centralized in the deep operations coordination cells. These cells support corps and EAC in planning, coordinating, and executing deep attack operations, including precision strikes, TMD, and the synchronization of associated air defense (AD) and aviation operations.

Depth and Simultaneous Attack 19: Communications Interoperability Between Joint and Coalition Forces. Future capabilities must include devices that provide automatic interfacing among joint and major coalition forces in support of deep attack operations.

Early Entry Survivability and Lethality

The early entry survivability and lethality battle dynamic is a concept that includes the ideas of innovative combinations of forces tailored to meet the challenge of any given contingency operation. These forces must be prepared to fight their way in, expand the battle space, enhance their own strengths, and preempt the enemy's strengths by dominating the use of information and using lightening speed. The applicable FCR follows.

Early Entry Survivability and Lethality 13: Real-Time Targeting. Early entry forces require the ability to receive and integrate real-time targeting data from advanced target-detection systems, including space-based early warning (EW) systems, into fire direction centers (FDC) to enable immediate response to provide effective lethal fires immediately on arrival.

Combat Service Support

This battle dynamic intends to improve the Armys ability to support the force from the continental U.S. It attempts to improve on the ability to use and reuse all classes of supplies, distribute supplies with total asset visibility, optimize soldier sustainment, and enhance force sustainment systems. In conclusion, the combat service support dynamic intends to enable the rapid tempo of the twenty-first century projection Army.

The Plan of How to Attain Force XXI

To develop the future requirements in terms of a vision and equipment, the Army uses the Concepts-Based Requirements System (CBRS). The CBRS is an overarching process that provides a design for identifying, prioritizing, and integrating a number of different areas of input. This process, which filters and synchronizes the development of the future force, is a result of combining requirements from--

-- The National Military Strategy (NMS).

-- Defense Planning Guidance (DPG).

-- The Joint Requirements Oversight Council (JROC).

-- The Joint Strategic Capabilities Plan (JSCP).

-- The CINC Integrated Priority Lists (IPL).

-- The Joint Warfighting Capability Assessment (JWCA).

-- The Army Long-Range Planning Guidance (ALRPG).

-- The Army Plan (TAP).

From the CBRS process comes the Army Modernization Plan (AMP) and the Army Science and Technology Master Plan (ASTMP). The AMP is an overarching plan for future development that provides information regarding specific systems that contribute to the achievement of modernization objectives.

The ASTMP is the Army's strategic plan for the science and technology effort dedicated to enabling the Force XXI concept.

The result of the CBRS and Force XXI concept process is the Army Digitization Master Plan (ADMP). The ADMP focuses on the development and support of an integrated digital information network that supports warfighting systems and assures C2 decision-cycle superiority over the enemy. This plan, written by the Army Digitization Office (ADO), addresses the Army's--

-- Requirements to organize, train, and equip a digitized force.

-- Unique requirements as a component of a joint or mulitnational force.

-- Functional requirements for sustaining the force from both a logistical and business perspective. The ADMP is intended to give guidance for the development of requirements for the future, while the Force XXI concept and the FCRs provide the vision.

Another equation in change includes the digitization systems planned to connect the national, joint, and Army elements into an integrated information network. Before describing Army systems, a brief look at the DoD system with which the Army must interface is provided for continuity.

The DoD portion of the information network is the Global Command and Control System (GCCS). It links all national and joint intelligence-gathering agencies and joint commands into one system. It provides a command, control, and communications (C3) network as well as an information internet that enables CINCs to gain information to make decisions and communicate those decisions to senior and subordinate headquarters.

The Army's requirement in the development of the information network is to develop a system that is interoperable with GCCS and that can provide information and intelligence from the lowest level of command to the highest. This becomes the data base for the relevant common picture. To do this in accordance with guidance documents, the Army designed the Army Battle Command System (ABCS).

To ensure the Army is synchronized with DoD in its development of Force XXI, the Army created the Modernization Campaign Plan, which consists of three axes. The Joint Venture axis, under Training and Doctrine Commands (TRADOC) leadership, will redesign the operational force. The TDA/Institutional Army axis, will redesign the nonoperational side of the Army. The ADO axis provides programmatic support for acquisition and assimilation of C4I capabilities into the force.

Vertical synchronization integrates the axes campaign plans in relationship to the overall Force XXI campaign plan by cross-walking subordinate missions with the higher mission. Horizontal synchronization involves the axes' campaign plans in relationship to each other. The plans are cross-walked to identify overlapping/dependant responsibilities, tasks, and requirements. Command and control structures are cross-walked to identify support relationships among the axes.

The Army Modernization Plan (AMP)

The AMP formally states the Army's funded plans for force development and modernization and clearly articulates goals for specific modernization efforts. This key document helps focus and discipline research, development, and acquisition (RDA) efforts. The AMP promotes better communication between the Army and industry and allows for early identification of programs that are not monetarily feasible.

The AMP provides information regarding specific systems that contribute to the achievement of modernization objectives. There are five modernization objectives:

1. Project and sustain the force.
2. Protect the force.
3. Win the information war.
4. Conduct precision strike.
5. Dominate the maneuver battle.

These objectives provide direction and focus for the balanced insertion of all technology into the force.

The AMP's goal is to provide Force XXI the capability to destroy, disrupt, and exploit an adversary's information systems while ensuring its own warfighters receive accurate, actionable intelligence and/or information. To do this, C4I planners must guide the technological development of a means of using a global grid to transport information between warfighters and supporters at all levels of warfare. The Army's part of that grid is the ABCS, whose architecture is intended to extend from the strategic installation (the main power projection platform), through the theater of operations, to the operational and tactical headquarters, and ultimately to the soldier on the ground.

Military communications systems aid the execution of C2 and supporting functions by providing rapid, reliable, and secure information interchange throughout the chain of command. A complete and interconnected system of communications must extend from the NCA, through the Chairman of the Joint Chiefs of Staff (CJCS), to combatant commanders (Commanders in Chief (CINCs)), commanders of service components, and all subordinate commanders.

To accomplish the goals for the communications portion of the Force XXI vision, there is an integrated framework for the digital battlefield that is based on three separate and distinct architectures. The Army Science Board (ASB) defines these as technical, operational, and system architectures. The operational architecture describes what to build. The system architecture describes how to build it. The technical architecture establishes the rules and standards to follow.

Part of the developing communications package is the use of space products, including navigation, position location, intelligence, terrain visualization, weather, communications, and early warning. These products help forces effectively and economically operate in the joint arena. They also allow swift interface with all services for complete integration of information, no matter the source.

Space-based communications systems are a principal capability to ensure global outreach of Army forces even while projecting power from home installations. The GCCS and ABCS architectures require end-to-end, protected, seamless, large-capacity, information-transfer, and processing capabilities for the warfighter whenever and wherever needed. Space-based communications provides just that kind of capability; it is the Army's tactical internet for the world.

The Army Science and Technology Master Plan (ASTMP)

The ASTMP strategy is to equip the force with the technological underpinnings required for decisive victory in the uncertain world of tomorrow. By implementing this plan, the Army can maintain a technological edge and continue to modernize weapons systems. The Army science and technology investment will ensure timely demonstration of affordable weapons system concepts that will meet warfighters' needs. Such systems will be responsive to force projection and diverse new-era threats. They will comprise a world-class network of government and private science and technology capabilities to maintain the Army's land warfare technology superiority, to exploit rapid advances in information technology, and to provide a smart-buyer capability.

To provide guidance to the science and technology community, the Army has established a set of two hundred STO, which state specific, measurable, major technological advancements to be achieved by a specific fiscal year (FY). Such advancements must be consistent with the funding available in the current year and comply with the program objective memorandum (POM).

The whole art of military effectiveness lies in the ability to move forces across a theater of operations in order to strike at decisive points, adapting as rapidly as possible to the ever-changing and unpredictable fortunes of war. War is a cycle of see, think, and strike in which adaptability, intelligence, speed, and cooperation are vital ingredients. The ideal adaption is one that can be generated in real time during the course of battle. This is the domain of artificial intelligence (AI) and can be regarded as the ultimate in logical mobility.

Within the increased use of weapons systems is the growing role of software in modern warfare. Software is probably the most important part of the entire system because software provides links to other systems and enables the systems to quickly manage information to the desired degree needed by Force XXI. Software even determines the communications support the force will need to provide seamless, reliable, and timely data exchange between users, regardless of specific communications systems. The ASTMP includes plans that require common software language and capabilities for all systems.

Software-intensive weapons can thus generate the need for speed in threat assessment. As tactical activity in war speeds up, the requirement for speed of decision generates a further need to trust intelligent systems. While at the same time, the human element will always be necessary to oversee analysis. However, humans are being progressively over obligated, marginalized, and obliged to depend on capabilities and flexibilities written into C^2 software. For example, there are so many competing demands on commanders for information and direction, a mechanism he can use to resolve conflicts and allocate priorities becomes essential.

The Army Digitization Office (ADO) Army Digitization Master Plan (ADMP)

General Colin Powell, in speaking of digitization, said--

> From the commander's perspective, information received should provide an accurate description of friendly, enemy, and neutral elements in an area of concern--the battle space. To provide the information detail and quantity required, a distributed data base needs to be created from information provided by all available sources. Intelligence, operational, logistical, and administrative information must be fused and distributed in such a way that it can be pulled from this global 'infosphere' on demand. [15]

The DoD created a digitization concept to guide each service to ensure joint interoperability. The Army's framework is called "The Enterprise Strategy," which reflects the global-based philosophy of the popular TV show "Star Trek." It addresses the Army's requirements to organize, train, and equip the digitized force, the unique requirements as a component of a joint or

multinational force, and the functional requirements for sustaining the force from both a logistic and business perspective. It is the guiding concept for the ADO.

The ADO developed and wrote the ADMP that addresses strategies, responsibilities, requirements, acquisition, experimentation methodology, joint and combined interoperability, and the management process that will transform the Army into a twenty-first century information-age force. It is focused on leveraging the power of people, information, and technology.

Digitizing the battlefield entails applying technologies to acquire, exchange, and employ timely information throughout the battle space that is tailored to the needs of each commander, soldier, and force supporter. The objective of the Army's digitization effort is to assure the superiority of the C2 system by providing warfighters with a horizontally and vertically integrated digital information network. This effort would ensure a simultaneous and consistent picture of the battlefield from soldier to commander at each level, as well as ensuring the Army is obtaining interoperability with its sister services and allied forces.

Because future battles will be fought at faster tempos with weapons systems that have greater ranges, are more accurate, and can respond faster to requests for future support, the challenge for system designers is to develop technology that can receive vast amounts of information across multiple communications channels while not becoming overloaded. System designs must explicitly account for information-management requirements and be capable of quickly and easily moving large amounts of data. If such a system cannot be developed, the reality of information dominance will not occur.

The Army must also account for the unique needs of all users and conform to a common set of standards for communications equipment, computer hardware, software, system protocols, data, and information representation. This is a huge requirement considering the number of users and their differing needs.

Army Battle Command System (ABCS)

The ABCS is the architecture the Army uses to move information and is the Army's umbrella system. It is an integrated system that enables all units to interface with their higher headquarters, receive the relevant common picture, and outpace the enemy through information dominance.

The ABCS is the integration of battlefield automation systems and communications that functionally link strategic (national interest), operational (corps and EAC interests), and tactical (division and below interests) headquarters. It is being built within the framework of the Army's technical architecture, which is fully compliant with the DoD technical architecture framework for information management.

The ABCS is intended to link the Army into a coherent, common, and instantaneous acting entity. It will use broadcast battlefield information as well as information from other sources integrated with real-time friendly and enemy situations into a digitized image that can be graphically displayed in mobile and heads-up displays. It will permit commanders at every level to share a relevant common picture of the battlefield scaled to their level of interest and tailored to their special needs. Commanders at the same echelon of command will simultaneously share a perspective of their position in relation to adjacent units.

Maneuver, CS, and CSS leaders will be horizontally linked by common information and, for the first time, will have a way of visualizing how they will execute an integrated support plan in the battle space. Individual soldiers will by empowered for independent action because of enhanced situational awareness, digital control, and a common view of the battlefield. The system will be user friendly and enable information on logistics, maneuver, AD warning, intelligence, and artillery to be readily accessed through pull-down information menus.

The tactical internet characteristic of the system will greatly enhance all battlefield operating systems, with the greatest potential payoff in the areas of intelligence, operations, and fire support

functions, because of its shared and immediate nature. This feature will be enhanced by the information available from the Army and joint intelligence systems, that feed into ABCS. This interneted system will enable commanders to detect and track enemy forces throughout a given battle space, while horizontal linkage will enable swift sensing, targeting, and firing to destroy the enemy before he even perceives he has been targeted. Commanders accessing intelligence data bases will have greater access to, and place greater reliance on, the counsel of Civil Affairs (CA), Psychological Operations (PSYOP), and SF assets. Even on highly technical future battlefield human intelligence (HUMINT) will often remain the only source of reliable information about the enemy. Improved locating devices and digitized sensor-to-shooter linkages will greatly improve the accuracy and responsiveness of fire support systems.

The ABCS consists of three subsystems, which have subsystems of their own. The ABCS includes--

1. The Army Global Command and Control System (AGCCS), which links to the GCCS and consists of--

-- The Standard Theater Army Command and Control System (STACCS), which is an EAC C2 system.

-- The Combat Service Support Control System at echelons above corps (CSSCS/EAC), which gives an up-to-date picture of the service support situation.

2. The Army Tactical Command and Control Systems (ATCCS), which links directly to the AGCCS, and consists of--

-- The Maneuver Control System (MCS), which is a system for maneuver unit commanders and staffs to use to plan operations and share information with all other systems and which provides a common battlefield picture from battalion to corps.

-- The All-Source Analysis System (ASAS), which is an intelligence system that collates information, identifies high-value targets (HVT) and high-payoff targets (HPT), provides a common enemy picture to all other systems, and receives and sends information to national and joint intelligence systems.

-- The Combat Service Support Control System (CSSCS), which consolidates and collates support data to integrate situational awareness within CSS mission areas.

-- The Forward Area Air Defense Command Control and Intelligence System ($FAADC^2I$), which is an integrated system of weapons, sensors, and command and control that provides C^2 and targeting information to AD weapons system at the division and below levels.

-- The Advanced Field Artillery Tactical Data System (AFATDS), which is an integrated fire support C2 system that receives target information from ASAS to coordinate all fires, including mortars, field artillery, cannon, missiles, attack helicopters, air support, and naval gunfire.

3. The Force XXI Battle Command Brigade and Below (FBCB2) system links to ATCCS and consists of--

-- The Brigade and Below Command and Control System (B2C2), which provides situational awareness and C2 to the lowest tactical echelons.

-- The Intervehicular Information System (IVIS), also known as Applique, which is basically made up of laptop computers intended for individual vehicles.

ASAS is a modular, tactically deployable, computer-assisted IEW processing, analysis, reporting, and technical control system. It provides automated intelligence and information management, including interface data handling. It consists of hardware and software modules that perform system operations management and security; communications processing and interfacing; input message processing; intelligence processing and reporting; target identification and nomination; and intelligence collection management. The speed with which ASAS can analyze and

collate raw data speeds the intelligence analysis process to meet the near-real-time requirements of the sensor-shooter links. It provides current IEW and enemy situation information for access and use by commanders and other ATCCS users. ASAS not only provides the warfighter with a dynamic intelligence picture of the battlefield, it is available to all the systems of ABCS and is interoperable with joint systems (such as Joint Deployable Intelligence Support System (JDISS)).

A new concept being investigated, called the Battlefield Awareness and Data Dissemination (BADD) Advanced Concept Technology Demonstration (ACTD), will be added to the existing systems once it is successfully developed. The system will allow the commander to design his own information system; deliver an accurate, timely, and consistent picture of the joint/coalition battlefield; and provide access to key transmission mechanisms and worldwide data repositories. To achieve all this, the system will use an expanded bandwidth (100 to 1,000 times greater) for multimedia information delivery down to battalion level. It will provide a smart-push/commander-pull server to access multiple data sources, including national and theater intelligence and operational and logistics information, among many other services. This added system will allow the commander to tailor his view of the battle space.

All of these capabilities will substantially increase the demands on intelligence and communications systems. The tactical internet will have to have the necessary interconnectivity of a system in near-real time. The components in the Army portion of such a system is the ABCS. Unfortunately, the system is only as fast as it slowest links--the Single-Channel Ground and Airborne Radio System (SINCGARS), the Enhanced Position Location Reporting System (EPLRS) radios, and the Mobile Subscriber Equipment/Tactical Packet Network (MSE/TPN). However,

"while the 'Tactical Internet' will substantially improve communications connectivity, the digital data load of the future is expected to exceed the capacity of this network." [16]

Future battlefields will be in a complex radio frequency (RF) environment. The design of the communications systems supporting digitization will have to balance such multiple factors as bandwidth requirements, spectrum availability, compatibility with other communications systems, and susceptibility to jamming. General Sullivan says that, "Success in the information age will go to those who have the courage to challenge themselves, who constantly innovate, and learn how to adapt as they go."[17]

The following comment by General William Hartzog, TRADOC Commander, voices a major factor that still threatens the attainment of the Force XXI vision.

> The Army has gotten the Applique computers (those mounted on the vehicles) to talk to the ATCCS systems in the laboratory but has yet to demonstrate that capability reliably in the field. Technically and theoretically, they're supposed to be able to do that, but what we're finding is [in the field] things don't always work the way they do in the laboratory.[18]

Applique computers can now talk to the ATCCS, but the underlying problem still exists for the system as a whole: the gateways between ATCCS components are too small for the amount of information that is required to travel through them. The gateway that has the biggest job is the MCS. There is also concern over whether the bandwidth, or pipe, of frequency modulated (FM) radios used among the Applique laptops is wide enough to handle the high volumes of data that will be transmitted across the tactical internet. The problem, explained by Major General William Campbell, is that--

> The Army is trying to mix commercial Internet software, designed for very wide bandwidths, with military communications systems, specifically the Single-Channel Ground and Airborne Radio System (SINCGARS) that have a very narrow bandwidth. The commercial products are designed to work on pipes that are 10 million bits per second wide. In comparison...Army systems are equipped with bandwidths between only 2,000 and 16,000 bits per second wide.[19]

Colonel Steven Boutelle went on to illustrate the dilemma--

> You're competing among people trying to do voice on it, other people trying to send overlays on it, other people trying to send [operations] orders, [and] some people trying to send free text messages. All of those are competing for that limited bandwidth, and that's the challenge.[20]

Engineers are also working on compressing the data that is transmitted in the available bandwidths. This work is known as the wavelet theory. Once available, it can compress transmissions as high as a 63:1 ratio.

Intelligence XXI Concept

The development of the intelligence portion of Force XXI, holds many challenges for the Army. The military intelligence (MI) branch must fully integrate with all potential users and contributors throughout each stage of Force XXI development. To ensure integration while developing Intelligence XXI, the MI branch divided the future challenges into four major categories: threat, new MI missions, concept development, and test and evaluation. The MI branch considers the information age a significant factor in the examination of these challenges. The MI branch's approach is represented in the phrase:

> Intelligence can never again stand as a separate entity. Only timely intelligence produced by synchronized collection efforts can allow the commander to see the battlefield, and act decisively.[21]

Accordingly, a successful intelligence battlefield operating system must be light, mobile, fully interoperable, and capable of providing precise relevant intelligence.

It is against this backdrop that the following intelligence warfighting concepts were developed:

-- The commander drives intelligence.

-- Intelligence will be fully synchronized with operations and force protection.

-- Intelligence will be conducted from split-based operations.

-- Intelligence will undergo near-real-time broadcast dissemination.

-- Intelligence will be implemented by forces tailored to specific missions.

Commanders must assume a central position in the intelligence process and pull from each echelon the precise intelligence necessary to fight and win. One of the features of the Intelligence

XXI system, as planned, is that commanders can tailor intelligence by filtering portions of the broadcasts they receive to focus on the reports that fulfill their intelligence requirements. This type of dissemination would permit internetting of echelons for data exchange, horizontally and vertically, thus enabling the simultaneous sharing of a common picture of the battlefield at all combat echelons.

Internetting requires interconnectivity, which depends on equipment, software, and communications links that make up or support a system. Unfortunately, interconnectivity of ARSOF intelligence systems with CF has not yet been addressed. In fact, the MI branch did not include the ARSOF intelligence section in the planning for intelligence systems until 26 November 1996. Also, MI branch briefings show SOF as a HUMINT asset passing intelligence exactly the same way as long-range surveillance (LRS) assets. Although coonsidering SOF and LRS as like units makes sense based on mission similarities, SOF does not have the same intelligence insertion point into the conventional army unit as LRS units. Also, SOF uses joint intelligence systems to report information. Commanders insert SOF into the corps or division through the special operations command and control element (SOCCE) within that headquarters operations section. Conversely, LRS assets are inserted into the intelligence section because they are commanded and given missions by the intelligence command or section.

SOF uses the JDISS; LRS uses ASAS. Currently, these two systems are not interoperable. However, there are plans for the ASAS Block II (ASAS II) system to be interoperable with JDISS. In fact, ASAS II will use JDISS software that will allow ASAS II direct exchanges with joint and national data bases. ASAS II will also contain GCCS software to enable smooth interconnectivity with national and joint intelligence sources. However, this still will not change the way SOF interconnects with the conventional unit headquarters.

Communications links is another factor in determining the smooth interoperability of the intelligence system to achieve the goals of Force XXI. The signal branch has the mission to support

intelligence systems with communications links. However, technology has allowed the intelligence branch to specify and procure systems that require faster and larger communications links. When Force XXI requirements of internetting were added to these already unacquired requirements, the signal branch very quickly got behind in its efforts to plan and procure communications systems that supported intelligence linkage requirements. Consequently, to keep up, the MI branch began specifying communications ports and linkage on its intelligence equipment. This has not set well with the signal branch, but it has given the intelligence community the ability to use its systems, in dire cases, without signal branch communications support. Due to necessity, the intelligence community now plans its intelligence operations considering the availability of communications assets.

Understanding that the intelligence branch has continued to accomplish its mission and has focused on developing a plan for intelligence in the twenty-first century, there still is a disconnect in interconnectivity between ARSOF and Army CF because of the lack of interface between the MI branch and USASOC. The following paragraphs examine the equipment and capabilities that the intelligence community will use.

The ASAS is the MI branch's base intelligence-providing system. It is the most likely to contribute to the necessary interconnectivity between ARSOF and Army CF. It is the only system that, when interoperable with joint intelligence systems (such as ASAS II), will allow ARSOF to provide information more directly to Army units. ASAS provides all-source intelligence fusion to gain a timely and comprehensive understanding of enemy deployments, capabilities, and potential courses of action. However, in the existing EXFOR system, the S2 must ask for information in the particular area that an SF element is watching, otherwise it will not be part of the relevant common picture.

The All-Source Analysis System II-Remote Workstation (ASAS II-RWS)--

-- Hosts JDISS software.

-- Provides full-situation development.

-- Contains common ABCS hardware and software.

-- Has multilevel security.

-- Interfaces with joint, national, and allied IEW systems.

-- Rapidly processes large message volumes.

-- Produces immediate HVT and HPT alarming and reporting.

-- Communicates via multiple communications means, including ultra-high frequency (UHF), very-high frequency (VHF), satellite communications (SATCOM), and mobile subscriber equipment (MSE).

-- Produces digital terrain/weather products.

-- Is capable of direct data exchanges with joint and national data bases.

The ASAS II-RWS maintains access to national intelligence sources is through continuous improvements to the Army Tactical Exploitation of National Capabilities (TENCAP) program. TENCAP provides intelligence from national to tactical levels. ASAS fuses information from multiple systems, including TENCAP, then distributes the information through a communications architecture.

Trojan Special-Purpose Integrated Remote Intelligence Terminal II (TROJAN SPIRIT II) systems are an integration of data processing, multiplexing, encryption, modulation, and radio frequency equipment. The system can operate over commercial and military SATCOM systems and can transmit and receive voice, data, and imagery between continental United States (CONUS) and outside of the continental United States (OCONUS) bases and deployed forces at data rates from 512 Kilobits per second (Kbps) to 1.544 Megabits per second (Mbps). The system interfaces with

Defense Secure Networks (DSN) 1 and 3 as well as joint and service intelligence systems at all levels. This system is another pathway for ARSOF to provide intelligence to the ASAS by electronic means, eliminating human interface. This is all based on the sending element using SATCOM.

The Digital Communications Satellite Subsystem (DCSS) encompasses the modulation, multiplex, coding, and processing equipment necessary to assemble various types of user data into a digital form suitable for transmission over a satellite link in both protected and unprotected modes. The terminal stores up to 90 megabits of user data. It is deployed as part of the Defense Satellite Communications System (DSCS) and essentially provides a unique wide band digital transmission capability. This system can become part of a pathway for an ARSOF element to input information, if there is a need to digitize the information, or it can store the information (for tactical reasons) in a satellite for future broadcast to the intelligence system.

These Intelligence XXI goals have been established, and there is an equipment-fielding schedule with an updating plan. But, there is no definable path that leads to the fulfillment of Force XXI requirements. That is, the paradigms identified for the Force XXI concept (seamless sensor-shooter linkage, real-time information, relevant common picture) are not fully supported by the Intelligence XXI concept. They are partially addressed by the warfighting concepts mentioned above. These paradigms are more fully supported by the phrase: *a successful intelligence battlefield operating system must be light, mobile, fully interoperable and capable of providing precise, real-time relevant intelligence.* (Emphasis added by author.)

A Synthesis of the Army's Position

The computer systems that are being created to realize the true concept of Force XXI and the internetting, or interoperability of these systems, is quite complicated and convoluted. In the interest of this thesis, it is appropriate to summarize the Army's position, explain the true complexity

of the intelligence interconnectivity issues of ARSOF and CF, and ensure all subordinate questions are answered sufficiently to support the thesis conclusion.

The normal modem speeds on a home computer are from 14.4 to 28.8 Kbps. The Force XXI concept requires that all units receive a relevant common picture, which is a map with appropriate up-to-date positions of friendly and enemy forces, terrain, roads, waterways, vegetation, and so on. To accomplish this feat requires about 13.2 million bits in order to portray a typical map image without friendly or enemy locations. To transfer this map at a speed of 9.6 Kbps would take 22.9 minutes transmission time, using 14.4 Kbps would take 15.28 minutes, and at 28.8 Kbps about 7.64 minutes. This assumes that the transmission line is consistently available for that amount of time without interruptions. If the effect of traffic loss on the line is added, it increases the time by 3.3 times. So the time required at 28.8 Kbps would be 25.2 minutes for one map view to be transmitted to one computer at one location. For Force XXI, the Army's C4I plan calls for an increase of transfer speeds of up to 100 to 1,000 times. If an increase of 100 times is realized, the required time to send the same picture would decrease to about 15 seconds. Unfortunately, the systems the Army now uses are not as fast as commercial home computers. The speed that information travels is based on the slowest link. The Army's slowest link is SINCGARS. The other most used equipment is the MSE. Figure 1 is a list of systems and their data transfer speeds. The speeds shown are today's speeds, but they do provide an idea of the challenges facing Force XXI digitization.

A brief examination of transfer technology illuminates other problems in the Force XXI concept that affect the ARSOF/CF intelligence interconnectivity. For instance, the use of asynchronous transfer mode (ATM) technology is one method that allows for a varied movement of information packets (file transfer protocol (FTP)) of information to be sent to a receiving address. The current method uses transmission control protocol/internet protocol (TCP/IP), which basically

System	Speed (Kbps)
ASAS II-RWS	19.2- 802.3
ASAS/CGS	2.4-16
ASAS/MSE	16
ASAS/SINCGARS	9.6
ASAS/SDR	14.6
ASAS/EPLR	0.96
EPLRS	7.2
LAN	10
JWICS	1 million (T3)
SINCGARS (FM radio)	7.2-14.6
TENCAP/SOF IV (broadcast)	1.2-19.2
TROJAN SPIRIT II	4.8-512

Figure 1. List of Army Systems and Their Information Transfer Speeds. [22]

creates a steady stream of information packets that go to all receiver locations until it finds the correct address. This creates a lot more traffic in communications lines than necessary and results in collisions of information packets. This increases information transfer time by a factor of 3.3. In other words, if the line is rated at 10 Kbps, the information will actually move at only 3 Kbps.

Other findings involve MCS and ATCCS. The EXFOR testifies that MCS cannot handle all the information that ASAS sends. Also, users must manually input enemy information into ASAS. Manual input is necessary to free up the net for extensive voice and data traffic. To confirm or deny that observation, the signal branch monitored Prairie Warrior 1996 and found that on a given communications line traffic peaked to the maximum capacity of 64 Kbps 13 times within the 8 hours of use each day.

The problems with ATCCS also illustrate the traffic jam concept. ATCCS sends information to subordinate systems one at a time via the TCP/IP method. Doing this decreases the amount of

information on the net, but that one packet of information must still circulate throughout the entire system, if necessary, to find the correct address.

The EXFOR also discovered that the system that produces the relevant common picture is degraded 75 percent while on the move. Add to all this the fact that information is only as good as how accurate it is and when it entered in the system. These detriments do not support the seamless sensor-shooter linkage in real time. It is obvious that these bugs must be worked out before the Army can realize the true vision of Force XXI with interconnectivity of all assets.

Currently, by Congressional mandate, CINCs are only responsible for planning two years ahead. This can create an interesting conglomeration of equipment and operating methods. How can the Army plan for the future without a long-term approach?

This is somewhat in evidence in the Joint Warrior Interoperability Demonstration (JWID). Each service participates to test its equipment to ensure interoperability with the other services. The problem is that each service is so interested in its own product that it loses sight of the necessity of interoperability with other services. Consequently each service addresses only what is absolutely necessary, and the interoperability of SOF that supports the services is addressed through the joint arena, not within each service.

Another area of concern to address to ensure the Force XXI concept becomes a working system is the map DATUM the military uses in coordinating the relevant common picture. Map DATUM relates to the accuracy of the map versus the actual shape of the earth. Each map is created using current available DATUM. Therefore, a map created in 1950 is not as accurate as one created today. This creates a disconnect in the maps for the different areas of the earth because not all areas have been mapped or use the same criteria. In fact, the US has mapped 65 percent of the earth with an accuracy of elevations taken every 100 meters, and 5 percent of the earth has been mapped every 30 meters. For the Force XXI relevant common picture requirement, 100 percent of the earth must

be mapped at one-meter intervals. The Defense Mapping Agency (DMA) says that the planned date for compliance to this standard is 2025.

Another factor in the investigation of the interface between ARSOF and CF, is fact that the Army does not view USASOC as part of the Army for the development of new equipment. The Army considers ARSOF part of SOCOM, because SOF has its own money with which to purchase equipment, and it conducts its own RD&A. The Army often forgets that ARSOF still relies on the Army for service common items. For example, the Army did not recognize USASOC's integration requirement in its planning until November 1996. In turn, USASOC created a battle lab to experiment with future concepts and there was a problem with the lab's focus. This was USASOC's fault, of course, but the Army did not recognize the SOF battle lab as even existing. Basically, the Army has committed *benign negligence* (author's italics) of ARSOF since SOCOM's inception.

Special Operations Forces XXI

Mr. Timothy G. Connolly, the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict (ASDSO-LIC), concerning support to SOF from the DoD perspective, says--

> Regarding intelligence support to SOF, which this office has sought to improve: There was a vigorous debate in recent years in the intelligence community at all levels, both military and national, about the types of intelligence that are needed for special operations--the scope, the detail, the difference between that kind of intelligence and what the 82nd Airborne, for example, needs for its missions. There was resistance in the intelligence arena to the notion that there was a need for specialized intelligence for special operations. But I have reason to believe that we've overcome that resistance, that there has been a recognition that SOF needs specifically what no one else needs and in a timeliness that perhaps other military operations can do without.[23]

Before going any farther, there is a need to explain SOF operational capabilities. SOF missions or capabilities include locating, recovering, or destroying strategic targets; obtaining critical intelligence; testing threat defenses, diminishing threat prestige; disorganizing, disrupting, or demoralizing threat troops; all to provide HUMINT, and divert important enemy resources from

the main battle area. SOF operates alone or with conventional forces to maximize the capabilities of both.

SOF missions are intelligence-dependent and intelligence-driven. This means that SOF requires intelligence to train for and execute missions; and the missions are executed to gather intelligence. They require immediate and continuous access to information from traditional and nontraditional sources. Moreover, SOF requires detailed national and theater intelligence products at the tactical level of execution, most often in near-real time.

SOF missions and collateral activities increasingly require interaction with diverse joint and multinational coalition forces along with a corresponding need to acquire and transfer large amounts of information reliably, securely, and in real time. Usually this is done using either high frequency (HF) or SATCOM communications links.

Before examining future SOF development planning, a short explanation of the command structure will separate and illuminate some issues that affect the interconnectivity of ARSOF with CF in Force XXI planning. SOCOM is the senior command of all SOF and is commanded by a four-star general who is a functional command CINC. This means he is not a warfighter, but he provides forces with special warfighting skills to other CINCs. SOCOM's mission is to provide combat-ready SOF in both peacetime and war for theater combatant commanders, American ambassadors and their country's teams, and other government agencies. The CINC of SOCOM (CINCUSSOCOM) carries out that primary responsibility by performing several supporting functions, which include developing and acquiring SOF-unique equipment, material, supplies and services.

Because of limited funding, the Congressional Committees on Appropriations directed that SOCOM work with all research activities to ensure they consider technology needs of the special operations when developing their base programs. Congress reiterated that the unique missions of

SOF require their capabilities be based on the leading edge of technology. Therefore. Congress expects development activities "to expend an appropriate amount of the technology base effort to identifying and developing technologies that have special operations potential."[24]

SOCOM's technology strategy is to monitor emerging technology relevant to SOF needs, participate in selected programs that relate to SOF technology development objectives, and execute selected high-priority projects to exploit emerging technology for near-term SOF application. A key thrust of this strategy is to urgently proceed with the prevailing objective to--

> increase the capability of assigned forces through the fielding of special operations-peculiar material meeting user requirements in the shortest possible time, i.e., aggressive use of prototyping.[25]

SOCOM's planned areas of modernization for ARSOF include--

-- Developing, operating, and enhancing an ARSOF intelligence automation architecture.

-- Providing ARSOF timely selected secondary imagery through the Special Operations Command Research, Analysis, and Threat Evaluation System (SOCRATES) network (which is being replaced by JDISS).

-- Developing and fielding the SOF intelligence vehicle (SOF IV).

-- Developing and fielding a lightweight man-portable system to directly receive near-real-time imagery at field locations.

-- Creating a lightweight collection and direction-finding system for SOF.

The deputy CINC of SOCOM, MG James C. McCombs, USAF, and the Chief of Staff of RD&A Technology Programs, Roles, and Responsibilities, directed all subordinate commands to identify and submit candidate technology projects to their parent service consistent with mission needs and SOCOM technical development objectives (TDOs). They were to establish procedures

to ensure cognizance of the parent service's and other services' and/or agencies' technological efforts that might be relevant to SOF missions.

SOCOM's Technology Development Program, with its list of prioritized TDO, reflects SOCOM's command and field perspective of operational deficiencies and future capability needs that typically require either a new technological application or an advanced technological demonstration. The TDOs are reviewed and updated every two years in conjunction with the POM process and are officially approved by CINCUSSOCOM. The TDOs provide focus to the command, as well as to technicians, engineers, and industrial representatives, on areas of technology that potentially can address SOF operational deficiencies and meet SOCOM's FCR objectives.

The equipment that SOCOM has chosen to make the mainstay of its connectivity are TENCAP, Single Channel Anti-Jam Manportable Terminal I (SCAMP I), SOF IV, and JWICS/JDISS. TENCAP is a broadcast system of intelligence information. SOCOM's interest in TENCAP is to exploit national system capabilities for SOF support, to train and educate both providers and SOF users on national system capabilities, and to influence new national system design and operations to benefit SOF needs.

The Joint Worldwide Intelligence Communications System (JWICS) is an intelligence receiver and distributor. SOCOM chose it because it enables SOF to connect directly with national and joint assets. Its capabilities for transfer are 1.544 Mbps video and 64 Kbps data, traditionally split into two 512 Kbps video channels and one 384 Kbps data channel.

SCAMP I is used for mutimedia services for the SOF community, including C^2 voice and data services, intelligence voice, data, and imagery services. SCAMP I will be the principle C4I medium for SOCOM in the year 2001.

SOF IV is a self-contained automated intelligence system that is interoperable with the theater Intelligence Data Handling System (IDHS), SOF intelligence systems, and JDISS, which is

the primary intelligence system for SOF. Its capability for transmission is 19.2 to 802.3 Kbps and it will be interoperable with ASAS II, which will allow direct data transfer from the joint level to the Army level.

Other systems that help to ensure the system is effective for SOF are Special Operations Forces Tactical Assured Connectivity System (SOFTACS), SOCRATES, and SOF IV. An additional system that can help with connectivity is the Improved SOF High-Frequency Manpack Radio System (ISHMRS). ISHMRS is a HF system that, unfortunately, is not yet reliable enough for data transmission. It only has a 300-baud transmission speed, and it does not maintain a continuous stream of information while in transmission. Thus, when it breaks up in transmission, data is lost, and the message confused.

SOFTACS provides assured connectivity between the Joint Special Operations Task Force (JSOTF) major subordinate commands, their major subordinates units, and other commands, as directed, in support of SOF missions. SOFTACS will be provided to ARSOF units and Navy SOF (NAVSOF) component organizations. SOFTACS provides communications through the means of multiband, multichannel super high frequency (SHF) SATCOM terminals; tropo-satellite support radio (TSSR) systems; digital circuit switches; remote trucking systems (RTS); tactical local area network (LAN) equipment; and message gateway servers.

SOCOM's efforts to plan and establish a focus are noted. However, that does not mean that all activities are truly focused as the plan states and as evidenced by the following comment from a SOCOM JDISS/SOCRATES conference in November 1996. "There exists a need for a disciplined approach, a clear statement of direction, a plan for getting there, a plan for the architecture, and GCCS is the driver but to where?"[26] So the plans continue to be worked and directed.

SOCOM wrote in its 1996 C4I plan that Special Forces Operational Detachment-A (SFODAs) (SF teams) will need high-capacity digital capabilities to support voice, data, imagery,

and video information in the future. The presently planned connection is to link with GCCS in rural environments and in the DSN and LAN/WAN in more urban environments. The plan appears to be effective for SOF and, in fact, does have the SOF community's approval. However, SOCOM's joint and national focus, coupled with other factors that have affected USASOC, has helped to create a disconnect in the basic and future communications interconnectivity between ARSOF and CF.

For the interface to be successful within this planned system, SFODAs must send information by SHF SATCOM to the intelligence analysis element. At this time, however, there is not enough room on the existing arranged SATCOM system for all the deployed SFODAs to use SATCOM. Consequently, procurement of a SHF bandwidth is a high priority in the C4I plan. Another plan is to establish a worldwide interlocking HF base station system that would allow SFODAs to contact a base station anywhere in the world. The base stations would then retransmit the information to the appropriate command headquarters based on the message address.

High-technology research and development continue to be the key to SOF modernization. SOCOM has identified the following specific programs for modernization: tactical UHF/SHF, manpack HF, deployable LAN, secure telephone/facsimile (FAX), JDISS, and deployable imagery. Special emphasis for the future is being given to development of improved mobility, flexible C2 systems, enhanced night-vision capabilities, and integrated communications systems for all forces at all levels of command.

The DoD requires SOCOM to plan for special operations and Army RD&A programs to be closely coordinated to prevent duplication of effort while taking advantage of shared capabilities. CINCUSSOCOM has directed all SOF to rely on a close partnership with service components for service-common equipment. This means that the ARSOF commander is required to ensure his staff maintains a close relationship with the Army equipment being developed and issued to conventional Army forces is also issued to ARSOF.

The SOCOM C4I planning document also called attention to the following issues. The J2 initiatives adhere to standards and a set of common applications and application versions. The SOCRATES baseline upgrade is to be a subsystem of JDISS. However, SOCOM's concern is for a disciplined approach with a clear statement of direction and plan, that is, it needs an action agenda for "getting there," while being interoperable and using JDISS-SOCRATES with the command LAN. SOCOM is concerned that GCCS is a main driver; but to where? Why access intelligence systems via JDISS? Where will the data bases be? What is the role of intelligence?

Overall, SOCOM leads the way to more interoperable systems and--

> fortunately, thanks to some superb leadership, our special operations forces have set a very high standard for interservice cooperation. They have also set the example for operational adaptability.[27]

SOCOM has also provided the required directives to cause SOF service commands to interface with their respective services to plan for interoperability now and in the future. There is however, a partial shortcoming, which is gradually being reduced through planning for the future. The shortcoming is generated by the requirements placed on SOCOM. When SOCOM was created it immediately faced interoperability problems. SOF had to be immediately able to operate with national agencies or any of the services based on the joint missions of which SOF is regularly a participant. Basically, SOCOM is required, by necessity, to buy both what is needed now and what is required for the future. By creating some staff sections to brainstorm the future needs, SOCOM has gradually gotten a hold on the future. However, the service SOF commands have not been so organized or forward thinking. USASOC, for one, has looked specifically to SOCOM for equipment development and future planning. Now Force XXI is slowly creeping up on ARSOF, and there is no plan or established relationships with the Army to create an effective plan in enough time to solve the interconnectivity issues.

ARSOF XXI

USASOC is commanded by a three-star general who is the senior ARSOF commander, but he is subordinate to the SOCOM commander. Although USASOC is an Army command, it is responsible to both the Army and SOCOM. USASOC looks to SOCOM for SOF-specific equipment and guidance; it looks to the Army for common equipment and guidance. USASOCs mission is to organize, train, equip, administer, educate, maintain combat readiness, mobilize, and deploy assigned Active Component (AC) and Reserve Component (RC) ARSOF to accomplish the assigned missions in support of the warfighting CINCs and JSOTFs.

The guidance the USASOC staff received in 1995 concerning future planning was to interact with the Army staff on the development of Force XXI and to synchronize planning. USASOC was included in the synchronization effort for Force XXI and the modernization of the Army, but in the end it did nothing that involved the interconnectivity of intelligence systems. USASOC has focused internally for the past seven to eight years since SOCOM came into existence, and the Army has considered ARSOF part of SOCOM. There has been no long-range plan requiring any interface with the Army except by SOCOM policy. Still, USASOC has only a C4 plan, not a C4I plan. Again, this is because SOCOM has a C4I plan and USASOC looks to SOCOM for guidance for long-term planning. In fact, USASOC considered the following information for their long-range research and development planning:

-- Defense Planning Guidance.
-- SOCOM planning guidance.
-- War games.
-- Integration and prioritization assessment.
-- Program Objective Memorandum.
-- Mission area assessment.
-- USSOCOM C4I plan.

The USASOC intelligence section (Deputy Chief of Staff Intelligence (DCSINT)) has been working to be included into future Army planning for almost two years. In November 1996 it was invited to participate in a planning conference. Prior to this latest change to the ARSOF/Army relationship, the Army had always said that SOF did not have a valid requirement for ASAS. Now the MI branch has changed its position and has included ARSOF in the ASAS II fielding, even though ARSOF must purchase the eight terminals from SOF funds. The Army will, however, purchase any future terminals for fielding with ARSOF.

Army CF and ARSOF do not have an interconnected path to fulfill Force XXI requirements. And, as mentioned above, USASOC has no C4I vision or plan. In addition, Army, or the MI branch, does not have a coherent plan to include ARSOF. Interestingly though, USASOC has received inquiries from the Army staff to see if the story is the same between Army and ARSOF.

For ARSOF to plan for Force XXI, it must keep Force XXI requirements in focus (seamless sensor-shooter linkage, real-time information, and relevant common picture). To move closer to creating a plan and effecting the required interconnectivity of Force XXI, ARSOF asked to participate in the Army's advanced warfighter experiments (AWE). The answer was that it could participate, but only if it brought its own equipment. That is difficult to accomplish and makes the experiment artificial, because ARSOF does not have the planned ASAS II terminals or any type of communications equipment, such as MSE or SINCGARs, with which to interface with Army CF. To make the experiment worthwhile, interconnectivity must closely resemble that which would exist in Force XXI and Intelligence XXI. That is a serious challenge, so ARSOF is scrambling to try to make the experience worthwhile without the Army's help.

The ARSOF intelligence system is required to be interoperable with an Army Force XXI division or higher command. Also, FM 100-25 directs ARSOF to support an Army corps or higher command within the SOF mission profile.[28] SOF has a requirement to use intelligence from

national and joint sources to plan missions based on where SOF missions are executed on the battlefield and with what other services or allied countries forces.

The bottom line is that to support the Army command by doctrine, SOF must provide near-real or real-time intelligence. Consequently, ARSOF must be able to send information through Army intelligence systems and request information through joint/national intelligence systems. This implies that ARSOF must either possess both Army and joint/national intelligence systems, or develop a system that is interoperable with both. However, it is difficult to develop a system with these characteristics when there is no interface between the intelligence system developer for the Army and ARSOF, which had been the case until November 1996. USASOC's modernization ideas continue to state that emphasis is needed in future intelligence systems on joint and combined interoperability, which is understandable since USASOC looks to SOCOM for equipment planning.

In addition to the continuing need for intelligence systems to push information down to tactical users from national and theater sources, ARSOF needs to pull up intelligence collected by tactical units. Therefore, there is a requirement for complete interoperability from the national level down to the tactical level and back again (vertically). There is a similar requirement to distribute and acquire intelligence between like-level units (horizontally). This is exactly what the Force XXI concept describes as the end state of the digitization of the battlefield. Unfortunately, ARSOF is not going to become a participant in this vision unless the interconnectivity between ARSOF and Army intelligence systems in Force XXI planning becomes a reality.

Along with the intelligence system, ARSOF must possess a communications system that allows interconnectivity with Army and joint/national communications systems. SOF's primary method for communication has been HF. However, HF is not a reliable transmission method for digital traffic. Consequently, SOF has attempted to expand the SOF channel size on SHF (such as SATCOM). If sufficient SATCOM bandwidth becomes available for all deployed SOF units, the

effectiveness of intelligence transmitted will increase because it will allow immediate intelligence input into JDISS. To this end, USASOC has determined that communications equipment must have the capability to operate separately and together with conventional Army forces, other services, and allied forces. Computers must be interoperable with supported and supporting activities using compatible hardware and software must be able to process multilevel security data, and be readily deployable from the office to the battlefield.

SOF IV is one answer to interoperability with the theater IDHS. In effect, the information must go from the SF team gathering the intelligence to their higher communications link, usually the battalion known as the forward operating base (FOB), then into JDISS to be accessed by the Army conventional corps or division through GCCS.

SOFTACS is a vehicle mounted SATCOM terminal. It is another alternative for termination of SF team transmissions. The result is the same, however. Intelligence is input into JDISS for distribution to joint and national sources, and the Army receives intelligence through GCCS. This requires the SF team to use SATCOM for interoperability with JWICS or JDISS, since HF is unreliable.

In Force XXI, ARSOF will have the ASAS II-RWS which is interoperable with JDISS. To ensure this interoperability, there must be an expansion of the SATCOM capability to transmit a larger volume of information, more often, for more SFODAs. This may require a dedicated satellite for SOF, but it is an issue that SOCOM is working.

To continue to explore possible interconnectivity links, the common ground station (CGS) or the deployable intelligence support element (DISE), which is part of the Army corps analysis and control element (ACE) in the intelligence section, could possibly provide the required link between the Army command headquarters in a direct enough manner to effect a real-time seamless shooter-sensor linkage.

The CGS terminates Joint Surveillance Target Attack Radar System (JSTARS) and UAV transmissions of enemy locations for transfer to the corps ACE. It is basically a retransmission apparatus and, theoretically, could retransmit the SF team's transmission, if by SATCOM, and route it to the corps' ACE or the SOCCE ASAS. If this is possible, it would surely require specific formatting and the CGS internet protocol address in the message. It might also require the use of the corps satellite. This is an alternative for technicians to investigate.

The DISE is another possible method for direct interface with Army command headquarters. The DISE receives intelligence from CONUS-based data sources or from initial-entry collection assets and is JDISS interoperable. If SFODA transmits intelligence into JDISS or TROJAN SPIRIT II systems, DISE will eventually get the information. The time lag is what is questionable and may not fit the real-time requirement.

In summary, USASOC and the MI branch both mention interconnectivity as issues for modernization, but it is not, in reality, planned or synchronized. It is easy to view the past with perfect vision, but it appears that the result of USASOC not being involved in Force XXI planning (to ensure the interconnectivity of intelligence systems between ARSOF and CF) is ARSOF units having to carry and maintain two intelligence systems--one system for joint interoperability and one for Army interoperability. This is not the intent of Force XXI.

Putting It All Together: A Force XXI Scenario

The Force XXI division's deep strike assets are Apache attack aircraft and a block II Army Tactical Missile System (ATACMS). The missle system's maximum effective range is approximately 300 kilometers. This implies that the division is a key user of corps, theater, national, and possibly joint intelligence. It also implies that the SFODA could be gathering

intelligence for the division and the corps and, therefore, would require a seamless real-time link to the division.

The SFODA is conducting special reconnaissance (SR) in a corps commander's area of influence 280 kilometers in front of the corps. The team observes enemy vehicles that meet the corps commanders priority intelligence requirements (PIR). The SR site relays the information to the mission support site (MSS) to the communications specialist who sends the information to the team's communications termination site at the FOB.

At the FOB, the staff S2 reads the information from the JDISS terminal as it is being sent to the senior headquarters. The information flows up the chain of command through the JDISS and then down from the joint task force (JTF) headquarters through subordinate headquarters to the corps headquarters. To do this, the JDISS had to be interoperable with the Army's ASAS.

At corps headquarters, the G2 analyzes the information and informs the commander. At the same time, the ASAS updates the relevant common picture. The Army field artillery tactical data system (AFATDS) recieves the information from ASAS that updates its relevant common picture, analyzes the information, and determines that the vehicles represent an HVT. The AFATDS then sends a message to the appropriate artillery unit, which destroys the vehicles by indirect fire.

These actions could take from minutes to hours. The requirement for information to move to the FOB and into JDISS before the division recieves it does not create a seamless sensor-shooter linkage. However, this scenario illustrates the convoluted path necessary to produce the sensor-shooter linkage between Army SOF and CF. Attaining the goal of real-time, seamless sensor-shooter linkage is not accomplished via this route.

---

[1]Wayne A. Downing, "Special Operations Forces: Meeting Tomorrow's Challenges Today," *Special Warfare Magazine* (January 1995): 2-4.

[2]Alvin and Heidi Toeffler, *War and Anti-War*, (New York:Warner Books. Inc., 1995): 302.

[3]Toeffler, *War and Anti-War*.

[4]Toeffler, *War and Anti-War*.

[5]Gordon R. Sullivan and Anthony M. Coroalles, "The Army in the Information Age." (Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College, March 31, 1995): 4.

[6]John D. Rosenberger, "A Year in the EXFOR," *Army* , Vol 46, No.11, (November 1996): 26-29.

[7]Rosenberger, "A Year."

[8]Morris J. Boyd and Michael Woodgerd, "Force XXI Operations," *Military Review*, (November 1994): 16.

[9]U.S. Army, *United States Army Posture Statement FY 96*, (Washington: Department of the Army, 1995): 52-54.

[10]U.S. Army, *Army Digitization Master Plan*, (General Gordon R. Sullivan and Colonel James M. Dubik)(Washington: Department of the Army, 1996): 6.

[11]William A. Owens, "The Emerging System of Systems," *Military Review* (May-June 1995): 15-19.

[12]U.S. Army, " FORCE XXI,"extract from *TRADOC Pamphlet 525-5, Chapters 3 and 4* (Washington: Department of the Army, August 1994).

[13]Gregory Fontenot (director, School of Advanced Military Studies, U.S. Army Command and General Staff College, Fort Leavenworth, Kansas) Brigadier General Morris J. Boyd and Major Michael Woodgerd, "Force XXI Operations," *Military Review*, (November 1994): 20.

[14]U.S. Army, *TRADOC Pamphlet 525-66, Operational Capability Requirements* (Washington: Department of the Army, 1995): 36.

[15]Richard F. "Riccardelli, "The Information and Intelligence Revolution", (General Colin L. Powell, " Information-Age Warriors," *Byte* (July 1992) 370.) *Military Review* (September-October 1995): 82-87.

[16]Michael I. Prevous, 'The Battle Command Support System: A Command and Control System for Force XXI" (Fort Leavenworth, KS: School of Advanced Studies, U.S. Command and General Staff College, 1995): 40-41.

[17]U.S. Army, *Army Digitization Master Plan*, (General Gordon R. Sullivan and Colonel James M. Dubik)(Washington: Department of the Army, 1996): 6-4.

[18]Sean D. Naylor, "Showtime, Officials Time", *Army Times* (November 1996): 12-14.

[19]Naylor, "Showtime."

[20]Naylor, "Showtime."

[21]Ira C. Owens, "Army Intelligence Operations in Force XXI," *Army* (October 1994): 145-149.

[22]Rod Ritter, "IEW, Communications and Automation System Architectures," (Fort Huachuca, AZ: Directorate of Combat Development, US Army Intelligence School, 1996).

[23]Glenn W. Goodman, "Special Report-Interview With Timothy G. Connolly, Principal Deputy Assistant Secretary of Defense (Special Operations and Low-Intensity Conflict) *Armed Forces Journal,* Vol 131, no. 4 (November 1993): 26-27.

[24]U.S. Army, *Army Science and Technology Master Plan*, 2 Volumes. (Washington: Department of the Army, 1995): F-2.

[25]U.S. Army, *Army Science and Technology Master Plan.*

[26]Thomas N. Sampson, "JDISS-SOCRATES Systems Update," Briefing given to the Senior Intelligence Officer (SIO) Conference, (Florida, 12-14 November 1996).

[27]David E. Jeremiah, Vice Chairman, Joint Chiefs of Staff, "Melding Special Operations with Forces of the Future," *Defense Issues*, Vol. 7, no. 7, Lecture Delivered at the Special Operations and Low-Intensity Conflict Symposium and Exposition (Washington: December 1991).

[28]U.S. Army, *Field Manual 100-25, Doctrine for Army Special Operations Forces* (Washington: Department of the Army, 1991).

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

Historical Background

Throughout this thesis, Force XXI is referred to as a vision and concept. The true spirit and intent of Force XXI can be summed up in a few words: a seamless sensor-shooter linkage, real-time information, and a relevant common picture. These terms illuminate the magnitude of this subject.

Without the interconnectivity to effect a seamless sensor-shooter linkage that produces a truthful relevant common picture that results in real-time information dominance over the enemy, Americans will die in future battles. This could happen if the Army cannot stay focused on the importance of interconnectivity, or if it does not exert that extra effort to ensure RD&A plans are thoroughly researched to include interconnectivity with all participants.

Within the Army, the MI branch dutifully looks to the Army for its guidance and focus. It also is struggling, like most services and branches, to make dollars stretch to cover requirements. The creation of SOCOM, which has its own budget, as an almost separate service causes a separation of ARSOF from the Army as a whole. SOCOM's mission to provide SOF for combat in joint and international environments led to giving guidance to USASOC to require ARSOF to become concerned with joint and national interoperability issues. This is especially important because this new headquarters was, for the first time, establishing relationships with its forces. While the Army specifically considers national assets external and a requirement above and beyond the normal and primary interconnectivity. All of these factors added together completes the requisite combination for "negligence" by the Army, the MI branch, and ARSOF. This may lead to the conclusion that

USASOC was justified in considering joint interoperability as the primary concern. That may be correct, but it did not release USASOC from dealing with the service issues of interconnectivity. SOCOM provided the directive to the SOF component of each of the services. It directed them to effect interface and to ensure interoperability and participation in planning and experimentation to stay abreast of the service modernization initiatives and how they were to interconnect with SOF. USASOC did not execute this requirement and is now behind on service-related interconnectivity and interoperability.

Interestingly, both ARSOF and Army intelligence established interconnectivity as goals for Force XXI. However, neither planned for its accomplishment. In fact, neither the Army MI branch nor ARSOF have established a path to fulfill Force XXI requirements as described in the TRADOC-established future capability requirements pamphlet.[1]

Early on in the life of SOCOM there was a realization that interoperability with joint and national assets was imperative in SOF's mission success. Consequently, SOCOM, with its SOF funds, proceeded to purchase equipment that was joint and national interoperable. In addition, SOCOM realized if it did not start investing in the future, technology would pass it by. So, SOF was required to invest in the present and the future at the same time. The result is that there was no real path planned for future development to support a future vision.

As time progressed, SOCOM and USASOC executed some planning, and USASOC presented the requirement to be interconnective in the areas of intelligence and communications. It appears that what was implied by those requirements was directed to joint and national levels, following SOCOM's lead. Consequently, Army interconnectivity was left out of planning and the vision.

What is troublesome is that USASOC was included in the synchronization effort for Force XXI, but apparently did not become an active member interfacing with the TRADOC team in charge of synchronizing Force XXI efforts. This means that USASOC has no long-range plan that includes

the interconnectivity of intelligence systems. Now, in an effort to catch up with the Force XXI development process, USASOC has requested to participate in the upcoming AWE. The Army's response was almost predictable considering the past interrelationship between the Army and ARSOF. The Army said, OK, but bring your own equipment at your own expense. That is not realistic, since ARSOF does not have the necessary equipment to replicate the Force XXI required interconnectivity. The late inclusion of ARSOF in the Intelligence XXI planning process reinforces the benign negligence the Army has perpetrated on ARSOF in the past. Again, not necessarily intentional, but obviously apparent.

USASOC itself had been focused internally since the creation of SOCOM primarily because of its focus on SOF and the associated requirements. The result is that USASOC has neglected its interrelationship with the Army. The USASOC commander directed all staff offices to interface with the Army for planning, back in 1995. But current bids show that the staff did not comply with the directive.

USASOC even created a battle lab, as the Army had done, to examine the SOF area of Force XXI future concept requirements and to develop twenty-first century SOF capabilities. Unfortunately, the battle lab became a special-project office. This might have been a simple case of the urgent supplanting the important, but whatever the cause, USASOC has no C4I vision or plan to interconnect SOF and CF.

The results of all of these perceptions, noncompliances, and negligence is that ARSOF is now saddled with two different intelligence systems that it is required to carry to the battlefield and maintain. However, there are ways to interconnect CF with ARSOF, although they are planned solutions to a perceived problem. The available methods are purely by happenstance and after-the-fact "finagling."

By effecting interconnectivity through indirect methods, many issues crop up to challenge the linkage to provide the requisite results of Force XXI paradigms. For instance, if the SOF SATCOM bandwidth is not expanded, as planned, it will not matter how many intelligence systems SOF has or the issues created by indirect methods; the information will not get to the appropriate commander and action unit in real time, or near-real time.

Methods of Intelligence Transfer

Chapter 4 illustrates the accumulation of generalized discoveries from the research. The scenario shows the actual stages and path that ARSOF intelligence must take to effect interconnectivity between ARSOF and conventional forces. This process could occur within seconds, hours, or never, depending on--

-- The amount of information.

-- The equipment's transfer speed capability.

-- The timing of the transmission.

-- Whether there are traffic jams occurring on the tactical internet.

-- The availability of space or the size of bandwidth on communications links.

-- The transfer protocol or method of addressing messages moved on the tactical internet.

-- Whether the receiver equipment is degraded during specific operations, such as movement.

-- Whether the intelligence officer has specifically requested SOF intelligence be added to his relevant common picture.

Required Connectivity

There are other methods to connect ARSOF and CF intelligence systems, but they are more circuitous and do not satisfy Force XXI paradigms. One method requires an SF team to send the information to a specific computer address located at a CGS.

Another method, is for the corps SOCCE to manually input the information into the SOCCE ASAS terminal. In twenty-first century warfare this will be a slow and unreliable method. Seconds will count more than they do today. The estimated time required for this would be from 30 to 45 seconds in the best case, assuming that ASAS computers can immediately assimilate the information, regardless of other information being simultaneously assimilated, and add the information to the data base or common relevant picture.

A SOCCE soldier at the corps operations center could also hand carry a printed copy of the information to the corps deep planning cell. In this method the estimated time for information transfer would be appropriately forty-five seconds. (This actually occurred in the FY96 AWE, Roving Sands exercise.) This is a reliable method, but is extremely slow in the twenty-first century sense of time because the information would not become part of the relevant common picture until it was entered into the ASAS.

Research Summary

To summarize the research for this thesis, it is best to review the subordinate questions. Does the Force XXI concept plan to interconnect the Army with national and joint intelligence-gathering assets? The Force XXI concept is explained in detail in Chapter 4, but the answer is yes, with the result being a relevant common picture of friendly and enemy forces on the battlefield, with completely interconnected intelligence systems. Force XXI; the contributing DoD synchronization axes; the GCCS; the Army's Modernization Campaign Plan, with the Force XXI synchronization matrix; and planned interoperability of ASAS with JWICS/JDISS ensure the Army is interconnected with national and joint intelligence systems.

Who is involved in the requirements process, and are SOF and CF interconnected? As of 26 November 1996, the Army, USASOC, and SOCOM are all part of the process. Army SOF and CF were not interconnected, but there is an opportunity for that issue to improve. Lieutenant General Peter J.

Schoomaker made it clear to all of USASOC that all offices should be talking to the Army about Force XXI and the Army After Next (AAN) concerning ARSOF input. The guidance exists; whether the execution will occur depends on every major section in USASOC. The intelligence section (DCSINT) is talking to the intelligence program manager (US Army Intelligence), but few others are. As of this writing, it is not occurring across the board.

Subordinate Thesis Questions

The following are the subordinate questions with answers to summarize. A quick list of these questions is in Figure 2 at the end of this discussion.

Does the Force XXI concept plan to interconnect the Army with joint/national intelligence assets? The GCCS and AGCCS create the link between national and Army assets.

Are SOF and CF interconnected in the requirements process? SOF is pursuing a requirements process that focuses on joint and multinational interoperability. Conversely, CF uses the Army concept-based requirements process to focus on Force XXI equipment development.

Are SOF and CF interconnected in the RD&A process? SOF is pursuing one set of equipment while the CF is pursuing another. There are now plans to make the two sets interoperable, but not interconnective, as defined by Force XXI.

Does the intelligence plan for RD&A interconnect SOF/CF? There is a plan by the MI branch, but it does not specifically include ARSOF. SOCOM has a plan for SOF to be interconnected via joint and national intelligence systems. The Army has no plan for ARSOF; it only has a CF intelligence plan for the future with no path of how to get there.

Is the Army planning to interconnect ARSOF and CF in the RD&A process? The Army has planned to purchase a number of ASAS terminals for USASOC. However, Force XXI paradigms on connectivity (sensor-shooter linkage, real-time information, and common relevant picture) will not be satisfied by this action.

Is SOCOM planning to interconnect SOF/CF in the RD&A process? The DCINC of SOCOM issued a directive to all subordinate commands that they are responsible for interfacing, planning, and monitoring service-specific RD&A for special operations applicability.

Are national and Army intelligence interconnected in RD&A? The AGCCS will interoperate with GCCS and then transmit the information to the MCS and ATCCS for further distribution.

Is the intelligence architecture currently interconnected? Actually, it is too soon to see any interconnectivity generated from the Force XXI concept. As for the existing interconnectivity, there is none except between SOF and joint and national assets. SOF has been spending funds to improve interconnectivity for the present as well as the future.

Currently, are there efforts to interconnect the intelligence architecture? There are some disconnects now. However, the extensive requirement for interconnectivity does not exist today as it does for the Force XXI concept.

Currently, are there problems with the intelligence architecture? There are no significant problems with the system based on today's requirements. However, for Force XXI there are significant problems with equipment, software compatibility, communications links, and systems architectures.

Do Force XXI plans show interconnectivity and compatibility? The basic concept of Force XXI is the interconnectivity and compatibility of systems that create a synergistic system that does more, faster, and with more accuracy than the enemy can. Basically, Army, national, and joint assets are interconnected by the virtue of the planned interoperability between ASAS and JWICS/JDISS.

Is ARSOF/SOF planning to meet with the Army to synchronize Force XXI plans? SOCOM has a C4I plan and is focused on joint, national, and allied interconnectivity. USASOC has no C4I plan and is following SOCOM's plan. Until November 1996, USASOC was not involved in Army Intelligence XXI planning and is still not involved. The MI branch is just increasing the requirements for future-issue equipment and requires USASOC to purchase the first eight terminals of ASAS II-RWS.

Is there a plan to integrate all parties and systems in the future? SOCOM is focused in one direction. USASOC is focused in two directions. And, the Army is focused in another direction. USASOC is caught in the middle between SOCOM and the Army. The results are that USASOC forces must deploy with and maintain two different intelligence systems that will, hopefully, eventually be able to communicate with each other (JDISS and ASAS II). There is no all-encompassing system planned or synchronized. The lack of a C4I plan at USASOC creates a situation that requires two intelligence systems to be available to USASOC units to ensure SOF information is integrated with the CF in the Force XXI paradigms: seamless, sensor-shooter linkage, real-time information, and the relevant common picture.

Is there a matrix to ensure parallelism between ARSOF and CF? Each plan is separate for SOCOM and the Army. The only synchronization of the two plans occurs at the JCS level for the development of GCCS and JDISS.

Do plans address speed, size, and security? National, joint, and Army systems security is an issue and is synchronized with all levels. Speed and size seem to be a side issue when considering the paradigms of Force XXI. To accomplish the Force XXI vision, speed and size of computers will be what is available off the shelf commercially and technologically.

Will the system being planned result in a seamless sensor-shooter link for ARSOF/CF? The link is planned and established, but probably not in real-time, which is an implied requirement for sensor-shooter linkages to effect the destruction of the target while under observation of the intelligence-gathering asset. In other words, when the SFODA sees the target, the results of reporting should be fast enough for the SFODA to also observe the destruction of the target if the commander desires to fire on the target.

Subordinate Question	Answer
1. Does the Force XXI concept plan to interconnect the Army with joint/national assets?	Yes
2. Are SOF and CF interconnected in the requirements process?	No
3. Are SOF and CF interconnected in the RD&A process?	No
4. Does the intelligence plan for RD&A interconnect SOF/CF?	No
5. Is the Army planning to interconnect ARSOF and CF in the RD&A process?	No
6. Is SOCOM planning to interconnect SOF/CF in the RD&A process?	No
7. Are national and Army intelligence interconnected in RD&A?	Yes
8. Is the intelligence architecture currently interconnected?	No
9. Currently, are there efforts to interconnect the intelligence architecture today?	No
10. Currently, are there problems with the intelligence architecture today?	Yes
11. Do Force XXI plans show interconnectivity and compatibility?	Yes
12. Is ARSOF/SOF planning to meet with the Army to synchronize Force XXI plans?	No
13. Is there a plan to integrate all parties and systems in the future?	No
14. Is there a matrix to ensure parallelism between ARSOF and CF?	No
15. Do plans address speed, size, and security?	Yes/No
16. Will the system being planned result in a seamless sensor-shooter link for ARSOF/CF?	No
17. Do plans address bandwidth?	Yes

Figure 2. Quick list of subordinate thesis questions.

Do plans address bandwidth? Bandwidth is addressed and has been found to be woefully inadequate. There is a plan to increase the bandwidth by 100 or 1,000 times for Force XXI. However, technical capabilities will decide the outcome of that plan.

Primary Thesis Question

It is appropriate to answer the primary thesis question: Will special forces (SF) teams be seamlessly connected to the intelligence systems of Army conventional forces (CF) in Force XXI?

Answering a question referring to the future usually requires an examination of the past. The results are then extrapolated to produce what will most likely happen in the future. In the case of Force XXI this method is extremely accurate, because with the CBRS what is planned and researched now will be what is acquired in the future.

To fully understand the true vision of Force XXI, the author analyzed the Force XXI concept and vision and then conducted a process to synthesize the concept to its smallest components. This process gave a thorough understanding of the interrelationships of all of the components. The most prominent characteristics that fully encompass the true vision of Force XXI are the paradigms of seamless sensor-shooter linkage, real-time information, and the relevant common picture.

When considering the thesis question in context of the research, it is necessary to consider the true meaning of interconnectivity within the Force XXI concept. The result of complete interconnectivity is a seamless movement of information among all participants that produces a relevant common picture and near-real time seamless sensor-shooter linkages. When full synergy of all forces is realized, information dominance will enable friendly forces to own the battlefield.

From this definition we see there are really two questions, one imbedded in the other. What is the true meaning of interconnectivity? And, are ARSOF and CF truly interconnected? Whether ARSOF and CF intelligence systems are interconnective is revealed by the quality and quantity of the interface between

the two. From the answers we get from these two questions we can derive the answer to the thesis question: there is **not** an identifiable or efficient interface for adequate interconnectivity, and there is **not** enough evidence to be convinced that there is intelligence interconnectivity when compared with the paradigms.

Correcting the problems of Force XXI interconnectivity will incur much work. Therefore, planners must work together to achieve consensus of opinion and commonality of equipment. Otherwise there will be chaos. This thesis poignantly illustrates that even if the military community can create measures, plans, directives, and visions to effect change, if the people involved do not ensure compliance, do not take action, or overlook the requirements, then soldiers will die.

Recommendations for Further Study

Interconnectivity is only one issue in the realization of the Force XXI vision. There are two critical issues concerning the maps used to produce the data base for creating the Force XXI relevant common picture. One is the actual depiction of map data. With what resolution or accuracy are maps to portray the actual ground? The other issue is, what is the area of the world that will need to be mapped to provide an full complement of world maps in the Force XXI data base?

Currently, only 65 percent of the earth's surface is mapped, and the typography was only recorded every 100 meters. This is not very accurate when considering that when the sensor-shooter linkage in a firing battery is attempting to destroy a target the rounds could land anywhere within a 100-meter radius or a 200-meter diameter.

Only another 5 percent of the earth has been mapped for every 30 meters. This means that in Force XXI, the Army could fight on only 70 percent of the earth's surface. Also, the available maps might not have the same scale and, therefore, could not be matched with each other. This means that the actual amount of area that could be used to produce a relevant common picture would, perhaps, be reduced to from 55 to 60 percent of the earth's surface.

As previously mentioned, bandwidth and internet protocol are critical areas for communications connectivity and will need further investigation. For example, what effect will they have on realizing the Force XXI vision?

Another area for further study is to determine how speed and the vast amounts of information available will affect commander leadership capabilities in Force XXI? At what will the Force XXI commander have to be better, and how will he train himself or obtain the training to be a successful twenty-first century battlefield commander?

---

[1]U.S. Army, *TRADOC Pamphlet 525-66: Operational Capability Requirements* (Washington: Department of the Army, 1995), 36.

BIBLIOGRAPHY

Articles

Babb, Joseph, G.D., LTC (Ret) US Army, Curt F. Weimer, LTC, US Army. "Prairie Warrior 96-Special Operations," Military Review (July-August 1996).

Boyd, Morris J., BG US Army, and Major Michael Woodgerd, US Army. 'Force XXI Operations," Military Review, vol LXXIV, no 11, November 1994, 17-28.

CTSA Architectures Directorate. MTN. M-22 Tactical Network. Information provided by USASOC DCSINT, Fort Bragg, NC, 1996.

Connolly, Timothy G. "Interview with Timothy G. Connolly, Principal Deputy Assistant Secretary of Defense (Special Operations and Low-Intensity Conflict," Armed Forces Journal (November 1993): 26-30.

Downing, Wayne A., GEN, CINC USSOCOM. "Special Operations Forces: Meeting Tomorrow'w Challenges Today." Special Warfare. vol 8, no 1 (January 1995): 2-10.

Emmett, Peter C. "Software Warfare," Joint Forces Quarterly (Summer 1994): 84-90.

Garner, Jay M. LTG "Space--'The Future of Force XXI.'" Army vol 44, no 11 (November 1994): 20-24.

Garrison, William F., MG USA (Ret). "A View From the Field: Army Special Operations Fores in the Current and Future Security Environments." Special Warfare vol 9, no 2 (May 1996): 8-15.

Goodman, Glen W., Jr. "A Special Report: Interview with Timothy G. Connolly, Principal Deputy Assistant Secretary of Defense (Special Operations and Low Intensity Conflict)." Armed Forces Fournal International vol 131, no 4, (November 1993).

Goodman , Glenn W., Jr. "JROC Guru. An Interview with Admiral William A. Owens." Armed Forces Journal International (February 1995): 36-37.

Jeremiah, David E. Admiral USN, Vice Chairman, Joint Chiefs of Staff. "Melding Special Operation With Forces of the Futur." Lecture delivered to the Special Operations and Low-Intenstiy Conflict Symposium and Explosition, Defense Issues vol 7, no 7, (December 1991).

Keller, Ulrich H. "Learning Leader XXI." Military Review (May-June 1995): 30-37.

Link, Charles D. MG, USAF. "21st Century Armed Forces--Joint Vision 2010." Joint Forces Quarterly no 13, (Autum 1996).

Sullivan, Brian R. "Special Ooperations and LIC in the 21st Century: The Joint Strategic Perspective." Special Warfare vol 9, no 2 (May 1996): 2-11.

Willis, G. E. "Special Report. Perry Reviews the Army of the Future." Army Times (November 18, 1996): 29-30.

Wilson, Thomas R. "Joint Intelligence and Uphold Democracy." Joint Forces Quarterly, #7, Spring (February) 1995, 54-59.

York, Ken. "Army Special Operations Command Pushes the Technology Envelope." Armed Forces Journal (November 1993).

Books

Davis, Stan and Bill Davidson. 2020 Vision. New York: Simon & Schuster, Inc., 188.

Fiery, Dennis. Secrets of a Super Hacker. Point Townsend, VA: Loompanics Unlimited, 1994.

Icove, David, Karl Seger, and William VonStorch. Computer Crime, A Crimefighter's Handbook. Sebastopol, CA: O'Reilly & Associates, Inc., August 1995.

Kramer, Melinda G. Glenn Leggett, David C. Mead. Handbook for Writers 12 Edition, 1995.

Sullivan, Gordon R., GEN US Army, and COL James M. Dubik, US Army, War in the Information Age, June 1994.

Toeffler, Alvin and Heidi, War and Anti War, Warner Books, Inc., May 1995.

Electronic Media/On-Line Sources

Office of the Secretary of Defense, Acquisition, Battlefield Awareness and Data Dissemination (BADD), Army Concept Technology Demonstration Master Plan, http://www.acq.osd.mil/at/BADD.html, 02 February 1997.

US Army. Army Acquisition Office. http://www.monmouth.army.mil/isma/.

_____. Army Digitization Master Plan '96,' Army Battle Command System (ABCS), http://www.ado.army.mil/admp/1996/05abcs.htm.

_____. Army Digitization Master Plan '96',3. Interoperability Framework. http:/www.ado.army.mil/admp/1996/03inter.htm.

_____. Army Digitization Office (18 January 1996). Army Digitization Master Plan. [On-Line]. http://www.ado.army.mil/adtoc.htm.

_____. Force XXI. http://204.7.227.75:443/f21home.html.

_____. Force XXI-TRADOC Pamphlets. http://204.7.227.67/force21/tradoc/pamphlets.htm.

_____. The ASAS Family. About the ASAS-All Source (ASAS-AS) Workstation. http://www.tsmasas.army.mil/asas-as.ht.

_____. The ASAS Block II Development. About the ASAS Block. http://www.tsmasas.army.mil/ccs.ht.

_____. The ASAS Family. About the Communications Control Set. AN/TYQ-40 (CCS). http://www.tsmasas.army.mil/asas-e.ht.

_____. The ASAS Family. About the ASAS-EXTENDED (ASAS-E). http://www.tsmasas.army.mil/asas-rws.ht.

_____. The ASAS Family. About the ASAS-Remote Workstation (RWS). http://www.tsmasas.army.mil.asas-rws-ht.

_____. The ASAS Family. About the ASAS-WARLORD (WL). http://www.tsmasas.army.mil/warlord.ht.

_____. Intelligence and Electronic Warfare Orientation. Version 1.0. CD Mr. Rod Ritter, Director of CIST Developments. E-mail: ritter%hual@huachuca-emh11.army.mil.

_____. Intelligence and Electronic Warfare Orientation. Versin 1.0. CD Directorate of Combat Developments. Intel XXI Package, USA Intelligence Center, 22 April 1996. Mr.Rob Ritter, Director of CIST Developments, E-mial: ritter%hual@huachuca-emh11.army.mil.

_____. Intelligence XXI. http://204.7.227.75:443/force21/lanes/intel/intel1.html.

_____. Intelligence XXI. http://huachuca-usaig.army.mil/intl_xxi/intl_xxi.html.

_____. Intelligence XXI. Home page, http:/www.tsmasas.army.mil/dcpages/dcdmain.html.

_____. Requirements Determination. Washington, DC: http://www-tradoc.monroe.army.mil/cmdpubs/reqdef.htm, 29 October 1996.

_____. TRADOC Pamphlet 525-5: Force XXI Operations. A Concept for the Evolution of Full-Dimensional Operations for the Strategic Army of the Early Twenty-First Century. Fort Monroe, VA, August 1994. bwebster@pica.army.mil, 6 September 1996.

_____. US Army Training and Doctrine Command: Requirements Determination. http://www.tradoc.monroe.army.mil/cmdpubs/reqdef.htm.

Interviews and Oral Histories

ARPI, Alexandria, Virginia
MG (Ret) David E. Baratto (dbaratto@arpihq.com).

US Army Command and General Staff College, Fort Leavenworth, KS.
COL Metz, 4th Infantry Division Brief, part of A308, Mobile Strike Force, 2 Feb 97.
LTC Curt Weimer, DJCO Instructor.
MAJ Stuart Schwark, CGSC Student, Military Intelligence Branch, Connectivity of SOF with Army conventional intelligence systems.
Ellen Godfrey, DAC DAO, definition of synthesis and analysis.

US Army Intelligence Center and School, Fort Huachuca, Arizona:
Mr. Rod Ritter, DCD, Intelligence systems architecture and information, DSN: 821-2010.

US Army John F. Kennedy Special Warfare Center and School, Fort Bragg, North Carolina.
COL Florer, Chief, DOTD, connectivity of ARSOF with conventional intelligence, DSN: 239-8206.
CPT Roosa, USAJFKC&S Battle Laboratory, 24 January 1997.

US Army Signal Center and School, Fort Gordon, Georgia.
Mr. Dale White

US Army Special Operations Command, Fort Bragg, North Carolina.
Mr. Jerry Reinhole, DCSINT, ARSOF involvement with Army concerning Force XXI intelligence interconnectivity and interoperability.

US Special Operations Command, Tampa, Florida.
MAJ Milo Gavin, USAF, SOJ5, Force XXI information, DSN: 968-5165.
LTC Paul Schaffer, integrationof SOF and conventional Army intelligence, DSN: 968-7013.

Government Publications

Barratto, David J. MG (Ret). Prairie Warrior 96, Special Operations Forces Lessons Learned Report, Fort Leavenworth, KS, 10 June 1996, approximately 75 pages.

Department of the Navy, Naval Research Laboratroy. Briefcase Multi-Mission Advanced Tactical Terminal (BMATT). Washington, DC.

Ritter, R. Intelligence and Electronic Warfare Brief, Directorate of Combat Development, US Army Intelligence School, Fort Huachuca, Arizona, 6 November 1996.

Ritter, R. All Source Analysis Systems Brief. Directorate of Combat Development, US Army Intelligence School, Fort Huachuca, Arizona, 6 November 1996.

Reinoehl, Jerry. Intelligence Systems Update. Special Forces Warrant Officer Advanced Course. 6 August 1996.

Sullivan, Gordon R., GEN USA and James M. Dubik, COL. War in the Information Age. June 1994.

US Army. All Source Analysis System (ASAS) Information Briefing. US Army Intelligence Center and School, IEW Systems Page, DCD, Fort Huachuca, Arizona. http://huachuca-dcd.army.mil/iewsys/asas.htm, 2 March 1997.

_____. United States Army Posture Statement FY96. Fort Monroe, VA: Office of the Chief of Staff, February 1995.

_____. Army Science and Technology Master Plan 2 vols, Washington, DC: Department of the Army, Deputy Assistant for Research and Technology, Defcember 1995.

_____. Command and General Staff College, Force XXI, extract from TRADOC Pamphlet 525-5 August 1994, Chapters 3 and 4. Issued as part of C310, Lesson 1, Fort Leavenworth, KS, 1996.

_____. Command and General Staff College Handout: Mobile Strike Force A308: Overview of Capabilities of the ATCCS Battle Functional Area Systems (BFAS). Program Executive Office C3 Systems. Fort Leavenworth, KS, 1996.

_____. "JWID 96" Briefing (Joint Warfare Interoperability Demonstration for 1996). US Army Special Operations Command, Fort Bragg, North Carolina, June 1996.

_____. The Deployable Intelligence Support Element (DISE), US Army Intelligence Center and School, Department of Combat Developments, DCD, Fort Huachuca, Arizona. http://huachuca.dcd.army.mil/CONCEPTS/dse.htm, 19 May 1995.

_____. Directive Number 70-4, Research, Development, and Acquisition, USSOCOM Technology Programs. MacDill Air Force Base, FL: United States Special Operations Command.

_____. Five Year Joint Venture Analysis Plan, Force XXI, LTC Z. Spears, approved by LTG J. E. Miller, US Army, Analysis Plan TRAC-SP-0395, 25 April 1995.

_____. Force XXI, America's Army of the 21st Century. Fort Monroe, VA: Officeof the Chief of Staff, Army, Lousiana Maneuvers, 15 January 1995.

_____. FM 100-7, Decisive Force: The Army in Theater Operations. May 1995.

_____. Information Dominance-White Paper, 1996.

_____. Requirements Determination. Fort Monroe, VA: US Army Training and Doctrine Command, http://www-tradoc.monroe.army.mil/cmdpubs/reqdef.htm (29 October 1996), March 1996.

_____. Science and Technology for Leaders of the 21st Century-A Short Course on the Science that Shapes the Modern Battlefield. Photonics Research Center. US Military Academy. Sponsored by the Army Research Office. http://www.usma.edu.Physicas/EE/Departments. Photonics Research Center slides.

_____. Army Science and Technology Master Plan, Fiscal Year 1996, vol 1. Washington, DC 20310-0103.

_____. The Army After Next Project, Emerging Impresssions. US Army Training and Doctrine Command, Deputy Chief of Staff for Doctrine, Fort Monroe, Virginia, 1996.

_____. TRADOC Pamphlet 525-5; Force XXI Operations; A Concept for the Evolution of Full-Diensional Operations for the Strategic Army of the Early Twenty-First Century. Fort Monre, Virginia, August 1994.

_____. TRADOC Pamphlet 525-66; Operational Capability Requirements. Fort Monroe, Virginia, 1 December 1995.

_____. Training and Doctrine Command (TRADOC) Pamphlet 525-66; Operational Capability Requirements, 1 December 1995, 36 pages.

_____. TROJAN SPIRIT II, US Army Intelligence Center and School, IEW Systems Page, DCD, Fort Huachuca, Arizona. http//huachuca-dcd-army.mi./iewsys/trjsprt2.trm. 2 March 1997.

_____. United States Army 1995 Modernization Plan, April 1995.

_____. United States Army Posture Statement, FY96. Presented to the Committees and Subcommittees of the United States Senate and the House of Representatives, First Session, 104th Congress. The Honorable Togo D. West, Jr., and General Gordon R. Sullivan, February 1995.

_____. US ASCO Command Architecture Program (CAP), Strategic Planning Process, Mission Area Analysis; A Precursor to the USSOCOM FY 98-03 Program Objective Memorandum. USASOC, Fort Bragg, North Carolina, July 1995.

_____. US Army Special Operations Command, Deputy Chief of Staff for Intelligence, DCSINT/G-2/S-2 Conference, 18-21 May 1996.

_____. USSOC C4I Architecture, US Army Special Operations Command, Fort Bragg, North Carolina, 1996, 12 pages.

_____. USASOC Force XXI Campaign Plan. Fort Bragg, North Carolina, 8 December 1994.

_____. USASOC: SOF Intelligence Vehicle. USASOC DCSINT, Fort Bragg, North Carolina, 1996.

_____. USASOC: US Army Special Operations Forces XXI Campaign Plan. Fort Bragg, North Carolina, 18 January 1995.

_____. US Army Special Operations Command: Funded Requirements (White, Non-Aviation). Fort Bragg, North Carolina, 1996.

_____. USASOC Integrated Process and Product Team (IPPT) for US Army AWE Division XXI ARSOF Participation. US Army John F. Kennedy Special Warfare Center and School, Fort Bragg, North Carolina, December 1996.

_____. USASOC Long Range Planning Guidance 1993. USASOC, Fort Bragg, North Carolina, 1993.

_____. US Army Special Operations Command: Research, Development, and Acquisition. Mr. Tony Gies, Material Integration Division, USASOC, DSSRI, Fort Bragg, North Carolina, 1996.

_____. United States Army Special Operations Command Strategic Planning Guidance, US Army Special Operations Command, Fort Bragg, North Carolina, 1996, 25 pages.

_____. USASOC: SOF 2020, Army 2010 Vision. LTG Schoomaker, Commander, USASOC, Fort Bragg, North Carolina, 1996.

US Department of Defense. Five-Year Joint Venture Analysis Plan: Force XXI. Analysis Plan TRAC-SP-0395. TRADOC Analysis Center, Fort Monroe, Virginia, 25 April 1995.

_____. JDISS-SOCRATES Systems Update. USSOCOM/SOJ2-S. CAPT (USN) Thomas N. Sampson, briefing at SIO Conference, Tampa, Florida, 12-14 November 1996.

_____. DoD Dictionary of Military and Associated Terms, as amended by JMTGMS through HMGTM-094-95, (Includes US Acronyms and Abbreviations and NATO Terms (English only), 23 March 1994.

_____. Science and Technology Strategy and the DoD Technology Plan, 1996.

_____. Office of the Assistant Secretary of Defense (Special Operations/Low Intensity Conflict). United States Special Operations Command 1996 Posture Statement. The Pentagon, Washington, DC, 1996.

_____. USSOCOM Budget FY1996. USSOCOM Office of Legislative Affairs, Director SOLA, Tampa, Florida, August 1995.

_____. United States Special Operations Command (USSOCOM), United States Special Operations Command Directive 70-4.

_____. US Special Operations Command, US Special Operations Command Technolgoy Overview, 1996.

_____. USSOCOM C4I Strategy Into the 21st Century. MacDill Air Force Base, Florida, US Special Operations Command, Directorate of Command, Control, Communciations, Computers, and Information Systems, June 1994.

United States Special Operations Command, SOF Vision 2020, 1996, 14 pages.

Monographs

Pierce, George M. II, CPT USAF. "An Analysis of Strategic Planning to Support the United States Special Operations Forces' C3 Interoperability," Masters Thesis for Logistics Management, Air Force Institute of Technology, Air University, September 1992, 60 pages.

Prevou, Michael I., MAJ. "The Battle Command Support System: A Command and Control System for Force XXI," School of Advanced Military Studies, US Army Command and General Staff College, Fort Leavenworth, Kansas, First Team AY 94-95, 41 pages.

Schmidt, Harold S., LTC US Army. "Contingency Communications Planning for the Force XXI Army, Strategic Research Paper, US Army War College, Carlisle Barracks, Pennsylvannia, 18 April 1995, 70 pages.

Sullivan, Gordon R., GEN and Anthony M. Coroalles, LTC. "The Army in the Information Age." US Army War College, Strategic Studies Institute, Carlisle Barracks, Pennsylvannia, 31 March 1995.

Terpeluk, William LTC, USAR. "Lessons From the Past and a Vision of the Future: Tactical Headquarters Requirements in Force XXI," US Army War College, Strategic Research Project, Carlisle Barracks, Pennsylvannia, 18 April 1995.

Winfield, W. Montague, LTC US Army. "The Impact of Information Age Technology on Leadership and Battleifeld Command, Control, and Communications (C3)," Study Research Project, US Army War College, Carlisle Barracks, Pennsylvannia, 15 April 1996, 25 pages.

INITIAL DISTRIBUTION LIST

Combined Arms Research Library
U.S. Army Command and General Staff College
1 Reynolds Avenue
Fort Leavenworth, KS 66027

Defense Technical Information Center
ATTN: DTIC/OCA, J Chivas
8725 John J. Kingman Road, Suite 0944
Fort Belvoir, VA 22060-6218

U.S. Army Command and General Staff College
Directorate of College Services
Mr. John Reichely
Fort Leavenworth, KS 66027-1352

U.S. Army Command and General Staff College
Department of Joint and Combined Operations
LTC C. F. Weimer
Fort Leavenworth, KS 66027-1352

COL E. Wayne Powell
12201 Timbercross Circle
Richmond, VA 23233-2280

CERTIFICATION FOR MMAS DISTRIBUTION STATEMENT

1. Certification Date: 6 June 1997

2. Thesis Author: Major Steven T. Shoemaker, U.S. Army

3. Thesis Title: Army Intelligence Interconnectivity in Force XXI

4. Thesis Committee Members Signatures:

Mr. John A. Reichley

LTC C. F. Weimer

COL E. W. Powell

5. Distribution Statement: See distribution statements A-X on reverse, then circle appropriate distribution statement letter code below:

(A) B C D E F X SEE EXPLANATION OF CODES ON REVERSE

If your thesis does not fit into any of the above categories or is classified, you must coordinate with the classified, you must coordinate with the classified section at CARL.

6. Justification: Justification is required for any distribution other than described in Distribution Statement A. All or part of a thesis may justify distribution limitation. See limitation justification statements 1-10 on reverse, then list, below, the statement(s) that applies (apply) to your thesis and corresponding chapters/sections and pages. Follow sample format shown below:

SAMPLE	Limitation Justification Statement	Chapter/Section	Page(s)	SAMPLE
SAMPLE	Direct Military Support (10)	Chapter 3	12	SAMPLE
SAMPLE	Critical Technology (3)	Sect. 4	31	SAMPLE
SAMPLE	Administrative Operational Use (7)	Chapter 2	13-32	SAMPLE

Fill in limitation justification for your thesis below:

Limitation Justification Statement	Chapter/Section	Pages(s)

7. MMAS Thesis Author's Signature: _____